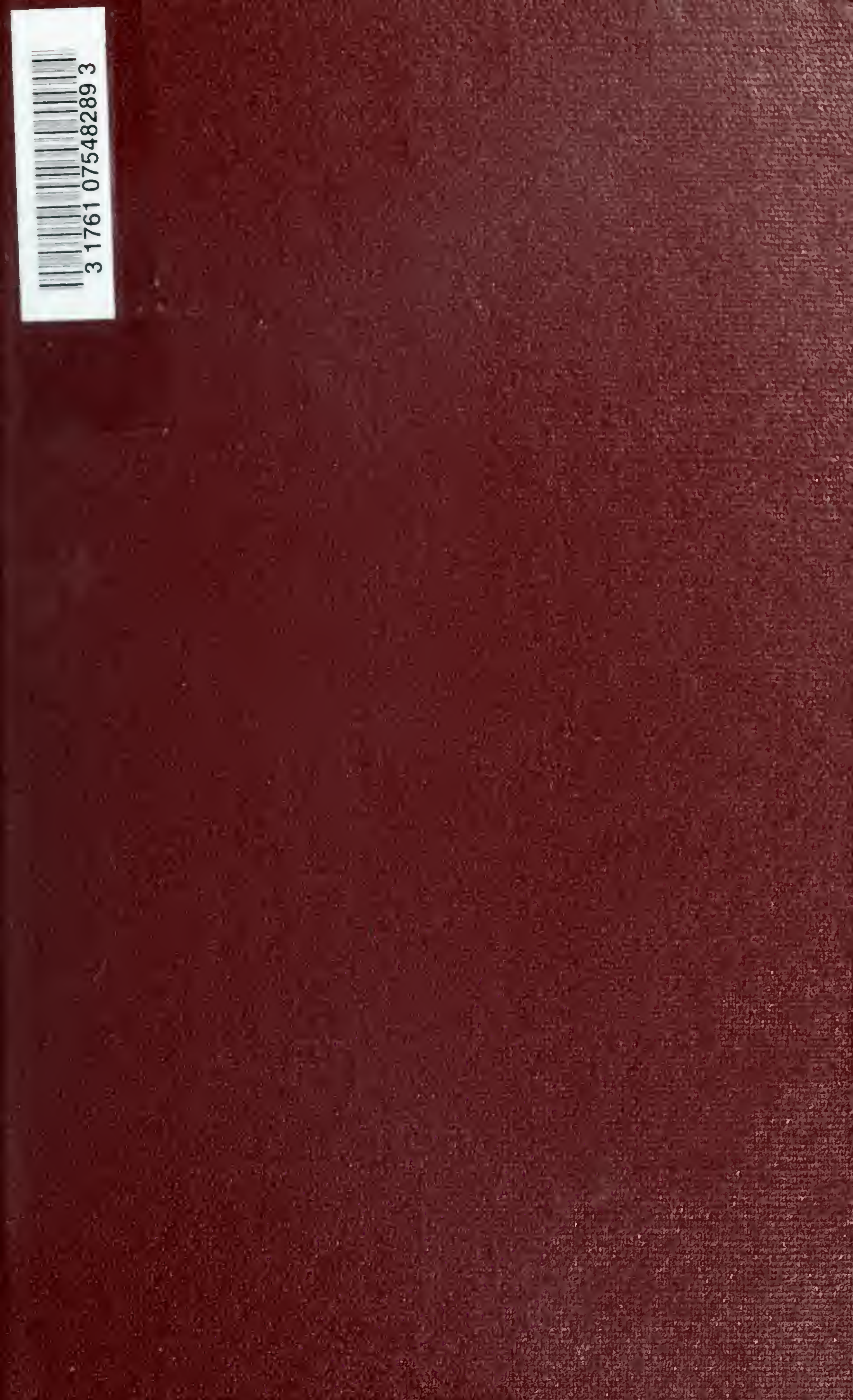

3 1761 07548289 3

INTRODUCTION

A LA

THÉORIE DES NOMBRES

ET A

L'ALGÈBRE SUPÉRIEURE

INTRODUCTION

A L'ÉTUDE

DE LA

THÉORIE DES NOMBRES

ET DE

L'ALGÈBRE SUPÉRIEURE

PAR

ÉMILE BOREL et JULES DRACH

D'après des

CONFÉRENCES

FAITES A L'ÉCOLE NORMALE SUPÉRIEURE

PAR

M. JULES TANNERY

SOUS-DIRECTEUR DES ÉTUDES SCIENTIFIQUES

PARIS

LIBRAIRIE NONY & Cie

17, RUE DES ÉCOLES, 17

1895

PRÉFACE

Pendant l'année scolaire 1891-1892, j'ai fait aux élèves de troisième année de l'École Normale quelques conférences sur l'Arithmétique et l'Algèbre. Je n'avais nullement l'intention d'exposer d'une manière dogmatique des parties de la science qui, sans doute, m'ont toujours vivement intéressé, mais que je n'ai point étudiées d'une façon particulière ; je voulais seulement diriger la curiosité de mes auditeurs vers des problèmes qui sont parmi les plus beaux de ceux que posent les mathémaques et des méthodes qui ont été trouvées ou perfectionnées par des hommes d'un génie singulièrement rare et pénétrant. Les progrès incessants de l'Analyse et de la Géométrie ne doivent faire oublier ni ces problèmes, ni ces méthodes. On sait assez, d'ailleurs, que les diverses branches des Mathématiques ne sont pas indépendantes et que ces propriétés du nombre entier, qui sont l'objet propre de l'Arithmétique et de l'Algèbre, interviennent dans bien des questions posées par l'Analyse. Il faut se rappeler enfin que l'enseignement des parties les plus élémentaires de l'Arithmétique et de l'Algèbre, de ces parties que l'on enseigne dans les lycées, suppose chez le professeur, s'il veut réellement dominer son sujet, au moins quelques vues sur les parties plus élevées de la science. Mon intention était simplement d'engager mes auditeurs à regarder de ce côté-là.

Dans les rares conférences que l'on peut dérober à la préparation des examens, il est très agréable d'enseigner ainsi, sans appareil logique, sans plan bien systématique, et dans une sorte de conversation. Les auditeurs s'y prêtent volontiers, et l'on sent assez qu'il n'est pas nécessaire de tout dire, de *développer* à tout propos ; on peut supprimer ici et là, ici, parce que c'est trop facile, là, parce qu'on serait entraîné trop loin, dans des régions même que le maître, qui n'a nulle raison pour s'en cacher, connaît mal et où il risquerait de s'égarer.

En Arithmétique, je me suis borné à expliquer sommairement la théorie des restes quadratiques et à ébaucher la division du cercle ; en Algèbre, je n'ai guère parlé que des équations abéliennes, en donnant parfois quelques indications sur d'autres sujets.

Il y avait cette année-là, à l'Ecole, deux élèves qui sont certainement parmi les plus distingués de ceux que j'ai eu l'honneur et la joie d'y rencontrer ; ils étaient venus des deux extrémités de la France, aussi différents qu'il est possible par la race et le tempérament ; ils s'y sont liés d'une amitié qui durera sans doute toute leur vie. M. Borel est déjà connu par de rares succès scolaires, par une thèse remarquable, qu'il vient de soutenir, et par quelques autres travaux. Sa place est assurément marquée parmi les mathématiciens qui feront honneur à notre pays.

Je crois bien que M. Drach ne tardera pas, lui aussi, à prendre une pareille place. Il a déjà acquis de nombreuses connaissances, dans des domaines variés ; il est de ceux qui se préoccupent avant tout du fond des choses, qui restent mécontents et inquiets tant qu'ils n'ont pas atteint le roc. Cette tendance philosophique de l'esprit est un danger quand elle travaille à vide, qu'elle n'est pas accompagnée de la connaissance des faits, et qu'elle engendre le mépris des vérités particulières, matériaux essentiels de la science ; c'est elle seule, malgré tout, qui préside à l'arrangement de ces matériaux.

Quoi qu'il en soit, mes conversations sur l'Arithmétique et l'Algèbre intéressèrent M. Borel et M. Drach, et quelques autres aussi, j'ose l'espérer ; mais je fus quelque peu étonné lorsque ces deux jeunes gens vinrent me proposer de les rédiger et de les publier ; j'eus beau leur représenter tout ce qu'elles avaient d'incomplet et de décousu : ils s'offrirent si obligeamment à les compléter et à les recoudre, ils insistèrent d'une façon si flatteuse et si affectueuse, que je me résolus, sans y réfléchir davantage, à les laisser faire. Ils se mirent donc à la besogne, travaillant ensemble, s'aidant et se critiquant l'un l'autre : M. Borel se chargea plus particulièrement de l'Arithmétique et M. Drach de l'Algèbre.

J'avais entièrement atteint mon but qui était, non d'enseiger, mais de faire apprendre. Il était très naturel que, dans ces conditions, ce que j'avais enseigné disparût quelque peu : c'est ce qui est arrivé, beaucoup plus que n'ont voulu se l'avouer, tout d'abord, les auteurs de ce Livre. Sans doute, j'ai, depuis, suivi leur travail, je l'ai parfois critiqué, et j'ai, par mes objections, contribué à éclaircir les idées de mes jeunes camarades. Mais j'étais engagé dans d'autres publications, et je n'ai pu consacrer à celle-ci tout le temps que j'aurais voulu : il vaut mieux qu'il en ait été ainsi : ce Livre en aura plus d'unité, et, qu'on me permette de le dire, plus de hardiesse.

M. Borel me reprocherait assurément de ne pas dire que, en parlant ainsi, c'est à M. Drach que je pense : c'est ce dernier qui avait assumé la plus lourde tâche, c'est lui surtout qui a fait œuvre personnelle. C'est à peine si, dans mes conférences, j'avais soulevé la question de la nature des *nombres algébriques*, c'est-à-dire des racines d'une équation algébrique entière à coefficients entiers, c'est à peine si j'avais indiqué comment, par l'emploi des congruences et des systèmes de modules, Kronecker avait pu fonder l'exposition de l'Algèbre sur une base purement arithmétique, et comment, à un point de vue tout autre, on pouvait regarder l'Algèbre, non comme un prolongement de l'Arithmétique, mais comme une partie de l'Analyse, le nombre algé-

brique n'étant qu'un cas particulier, nettement défini d'ailleurs, de l'irrationnelle générale. Mais il suffisait d'esquisser le problème pour que M. Drach s'y attachât, et le dernier point de vue, si parfaitement légitime qu'il soit, ne pouvait manquer de choquer un esprit aussi philosophique que le sien, par la façon dont on y fait appel à des éléments transcendants, bien éloignés de ce nombre entier, dont il semble que la considération doive suffire à la construction de l'Arithmétique et de l'Algèbre.

Le mode d'exposition auquel il a été amené par le désir de réduire à ce qui est indispensable la construction de l'Arithmétique et de l'Algèbre consiste essentiellement à regarder les nombres algébriques, aussi bien que les nombres entiers positifs ou négatifs et les nombres rationnels, comme des *signes* ou symboles, *entièrement définis* par un petit nombre de propriétés posées *a priori* relativement à deux de leurs modes de composition.

On part ainsi d'hypothèses bien déterminées qui n'impliquent point de contradiction, comme le montre l'étude de leurs conséquences. Cette étude conduit à quelques-uns des résultats que l'on doit à Kronecker, résultats que l'on peut résumer en disant que *le calcul dans lequel interviennent des nombres algébriques est identique à un calcul de polynomes à une variable, à coefficients entiers, dans lequel on néglige les multiples d'un polynome déterminé*. L'établissement de cette proposition, en partant des éléments, fait l'objet du chapitre III ; la nécessité de donner des règles pratiques pour effectuer le calcul dans un domaine algébrique amène, dans le chapitre IV, à exposer d'une manière nouvelle la théorie célèbre créée par Galois. C'est dans cette théorie que l'on doit d'ailleurs chercher le véritable fondement de l'Algèbre, telle que l'auteur l'a comprise, et la justification du mode de construction qu'il a adopté.

Il est à peine utile d'ajouter que ce mode de construction est purement logique, c'est-à-dire indépendant de toute notion expérimentale et en particulier de la notion de grandeur. Les

résultats acquis présentent néanmoins, au point de vue pratique, un certain intérêt : comme l'explique M. Drach, « il existe, en effet, des éléments géométriques, mécaniques ou physiques tels que l'on puisse établir une correspondance univoque et réciproque entre ces éléments et les symboles considérés ou une partie d'entre eux, ces éléments se composant d'ailleurs avec eux-mêmes de la même manière que les symboles correspondants ».

Lorsque M. Drach m'écrivit pour la première fois sur les sujets qui précèdent, au commencement de l'an dernier, j'eus tout d'abord, je l'avoue, quelque crainte à le voir jongler ainsi avec des symboles qui me semblaient vides de tout contenu ; je me suis persuadé, en y réfléchissant, qu'il y avait surtout, dans cette crainte, des habitudes d'esprit dont je ne parvenais pas à me défaire, et que, en réalité, elle était peu fondée.

Ce qui précède suffira, je l'espère, à convaincre le lecteur que si ce livre a quelque valeur, c'est à M. Borel et à M. Drach qu'il faut en reporter le mérite : c'est malgré eux que je le dis, mais je dois au lecteur la vérité. Si d'ailleurs, comme ils le croient, j'ai réellement contribué à leur inspirer le goût de la science, cela me suffit amplement.

Paris, le 16 juillet 1894.

Jules TANNERY.

TABLE DES MATIÈRES

PREMIÈRE PARTIE

THÉORIE DES NOMBRES

DEUXIÈME PARTIE

ALGÈBRE SUPÉRIEURE

NOTES

La rédaction de la première partie (*Théorie des nombres*) est due à M. Borel ; celle de la seconde (*Algèbre supérieure*), à M. Drach.

THÉORIE DES NOMBRES

PREMIÈRE PARTIE

THÉORIE DES NOMBRES

CHAPITRE PREMIER

PROPRIÉTÉS GÉNÉRALES DES CONGRUENCES

I. — Définitions et propriétés élémentaires.

1. On dit que deux nombres entiers, positifs ou négatifs, a et b sont *congrus* suivant le *module* positif m, lorsque la différence $a-b$ est divisible par m; c'est-à-dire lorsque l'on a

$$a = b + mq,$$

q étant un nombre entier (positif ou négatif). Si a et b étaient positifs et b inférieur à m, cette égalité exprimerait que b est le reste de la division de a par m. Nous conviendrons de dire, dans tous les cas, que a et b sont restes ou *résidus* l'un de l'autre par rapport au module m.

D'après cette définition, un nombre a a une infinité de résidus, compris dans la formule générale $a + mq$, où q désigne un entier quelconque, positif, nul ou négatif. Parmi ces résidus, il y en a toujours un et un seul qui est positif ou nul et inférieur à m; on l'appelle *résidu minimum*; dans le cas où a est positif, c'est le reste arithmétique de la division de a par m. Il y a quelquefois avantage à considérer une autre espèce de résidus

minima : il y a toujours un résidu compris entre $-\frac{m}{2}$ et $+\frac{m}{2}$, pouvant atteindre cette limite supérieure dans le cas où m est pair ; on l'appelle le *résidu minimum absolu* ; c'est celui dont la valeur absolue est la plus petite.

Pour que deux nombres soient congrus, il est évidemment nécessaire et suffisant que leurs résidus minima soient égaux. Or il est clair que le résidu minimum peut avoir seulement m valeurs distinctes : $0, 1, 2, 3, \ldots, m-1$. Considérons m nombres : a_1, $a_2, \ldots, a_m$ tels que deux quelconques d'entre eux soient *incongrus*, c'est-à-dire non congrus, suivant le module m ; leurs résidus minima seront tous différents ; ce seront donc nécessairement, abstraction faite de l'ordre, *tous* les nombres $0, 1, 2, \ldots, m-1$. On en conclut qu'un nombre quelconque x est congru à l'un des nombres $a_1, a_2, \ldots, a_m$.

L'ensemble de ces m nombres constitue ce que l'on appelle un *système complet de restes incongrus suivant le module* m ou, plus brièvement, *un système complet de restes* (mod. m). Le système complet de restes le plus simple est formé précisément des m nombres $0, 1, 2, \ldots, m-1$. Nous verrons plus tard l'intérêt qu'il peut y avoir à considérer d'autres systèmes complets de restes jouissant de propriétés particulières.

Ces notions très élémentaires ont néanmoins leur importance dans bien des questions de Mathématiques. Considérons par exemple l'expression $\operatorname{tg}\frac{k\pi}{m}$; nous savons que sa valeur ne change pas lorsqu'on augmente ou diminue l'entier k d'un multiple de m. Si l'on donne à k toutes les valeurs entières, cette expression prendra donc seulement m valeurs distinctes ; on obtiendra toutes ces valeurs en prenant pour k successivement m nombres formant un système complet de restes (mod. m).

Si h désigne aussi un nombre entier, $\operatorname{tg}\frac{h^2\pi}{m}$ est égal à $\operatorname{tg}\frac{k\pi}{m}$ lorsque h^2 est congru à k suivant le module m, et dans ce cas seulement.

Nous aurions pu, au lieu de $\operatorname{tg}\frac{k\pi}{m}$, considérer l'expression $\cos\frac{2k\pi}{m} + i\sin\frac{2k\pi}{m}$, qui joue un grand rôle en analyse. Elle donnerait lieu à des remarques analogues.

On voit par ces exemples, qu'on pourrait multiplier, l'importance que peut avoir l'étude systématique des rapports qui existent entre des nombres congrus ou incongrus suivant un module déterminé. C'est l'étude de ces rapports qui constitue la théorie des congruences dont nous allons exposer les éléments.

2. Il importe tout d'abord d'adopter une notation abrégée pour écrire que deux nombres a et b sont congrus par rapport à un module m. Nous adopterons la convention indiquée par Gauss et consacrée par l'usage et nous écrirons

$$a \equiv b \quad (\text{mod. } m).$$

Cette relation s'appellera une *congruence*. La notation choisie a l'avantage de mettre en évidence les analogies très grandes qu'il y a entre les congruences et les égalités ordinaires. On peut en effet soumettre les congruences de même module à presque toutes les opérations qui sont légitimes avec les égalités. Nous nous bornerons à énoncer ici ces propriétés ; elles se démontrent immédiatement en remplaçant chaque congruence telle que

$$a \equiv b \quad (\text{mod. } m),$$

par l'égalité correspondante

$$a = b + mq.$$

Il est clair, tout d'abord, que si l'on a

$$a \equiv b \quad (\text{mod. } m),$$
$$b \equiv c \quad (\text{mod. } m),$$

il en résulte

$$a \equiv c \quad (\text{mod. } m).$$

Si l'on désigne par λ, λ', λ'' des nombres entiers et si l'on a

$$\left\{\begin{array}{l} a \equiv b \\ a' \equiv b' \\ a'' \equiv b'' \end{array}\right. \quad (\text{mod. } m),$$

on a aussi

$$\lambda a + \lambda' a' + \lambda'' a'' \equiv \lambda b + \lambda' b' + \lambda'' b'' \quad (\text{mod. } m).$$

En particulier on peut ajouter ou retrancher membre à membre deux congruences de même module ; on peut aussi faire passer un terme d'une congruence d'un membre dans l'autre, par la même règle que pour les égalités.

Il est également permis de multiplier membre à membre deux ou

plusieurs congruences de même module ; des congruences écrites plus haut, par exemple, on déduit

$$aa'a'' \equiv bb'b'' \pmod{m},$$

et plus généralement

$$a^n a'^{n'} a''^{n''} \equiv b^n b'^{n'} b''^{n''} \pmod{m},$$

n, n', n'' étant des exposants entiers et positifs.

En combinant ces diverses propositions, on voit qu'elles se résument dans la suivante, dont elles ne sont que des cas particuliers : *Si $f(x, y, z, \ldots)$ est un polynome entier à coefficients entiers par rapport aux lettres x, y, z, ..., si de plus on a*

$$\left\{\begin{array}{l} a \equiv \alpha \\ b \equiv \beta \\ c \equiv \gamma \\ \ldots\ldots \\ \ldots\ldots \end{array}\right. \pmod{m},$$

il en résulte

$$f(a, b, c, \ldots) \equiv f(\alpha, \beta, \gamma, \ldots) \pmod{m}.$$

Mais, à l'inverse de ce qui a lieu pour les égalités, il n'est pas en général permis de diviser par un même nombre les deux membres d'une congruence, même dans le cas où ils sont exactement divisibles (s'ils ne l'étaient pas, cette opération n'aurait *pour le moment* aucun sens). Par exemple, on a

$$18 \equiv 6 \pmod{12}$$

et on n'a pas

$$9 \equiv 3$$

par rapport au même module.

Un examen attentif de cet exemple particulier suffit à indiquer comment on doit traiter le cas général. Si l'on a

$$a \equiv b \pmod{m},$$

cela signifie que $\dfrac{a-b}{m}$ est un nombre entier ; on ne peut pas en général conclure de là qu'il en est de même de $\dfrac{a-b}{mq}$, q étant un diviseur commun de a et b. Cette conclusion n'est légitime que si m et q sont premiers entre eux ; car, dans ce cas, $a - b$ étant divisible par deux nombres premiers entre eux, est divisible par leur produit.

On a donc le droit de diviser les deux membres d'une congruence par tout nombre premier avec le module et qui les divise exactement. (Nous

verrons plus loin comment on peut lever cette dernière restriction, en faisant une convention spéciale). En particulier, *si le module est un nombre premier*, les nombres qui ne sont pas premiers avec le module sont *congrus à zéro* par rapport au module, ou, plus brièvement, *nuls* suivant ce module et on a cet énoncé, tout à fait pareil à celui auquel on est habitué en arithmétique et en algèbre : *La division par zéro seule n'est pas permise.*

Dans le cas où m n'est pas premier, on voit très facilement que, si l'on désigne par δ le plus grand commun diviseur de m et de q, la congruence

$$a \equiv b \qquad (\text{mod. } m)$$

entraîne

$$\frac{a}{q} \equiv \frac{b}{q} \qquad \left(\text{mod. } \frac{m}{\delta}\right).$$

Si, en particulier, un nombre q divise a, b, m, on a $\delta = q$ et

$$\frac{a}{q} \equiv \frac{b}{q} \qquad \left(\text{mod. } \frac{m}{q}\right).$$

3. Nous nous sommes appuyés sur ce qu'un nombre divisible par plusieurs autres premiers entre eux deux à deux est divisible par leur produit.

La démonstration que l'on donne habituellement de cette proposition repose comme on sait sur le théorème : *un nombre qui divise un produit de deux facteurs et qui est premier avec l'un d'eux divise l'autre.* Cette dernière proposition se déduit de la théorie du plus grand commun diviseur. Il ne sera pas sans intérêt d'en donner ici une démonstration directe, qui est due à *Poinsot* (*), et qui nous conduira naturellement à d'autres propriétés très importantes.

Considérons la suite des multiples d'un nombre entier positif a,

$$0, a, 2a, \ldots, ma, \ldots$$

et divisons les termes de cette suite par un nombre entier positif m. Il est clair que ces restes se reproduiront périodiquement de m en m, mais la période peut être plus courte. Soit h *le plus petit nombre tel que* ha *soit divisible par* m, ha sera le plus petit commun multiple de a et de m ; h termes consécutifs seront toujours incongrus

(*) Dans un livre récent sur les éléments de la théorie des nombres, M. Bachmann a appelé l'attention sur la signification de la démonstration de Poinsot.

(mod. m) : en effet, si ka et $k'a$ étaient congrus (mod. m), leur différence $(k - k')a$ serait divisible par m, ce qui, par hypothèse, ne peut avoir lieu lorsque $k - k'$ est plus petit que h. Cette différence, au contraire, est évidemment divisible par m lorsque $k - k'$ est divisible par h ; les restes se reproduiront donc de h en h et la période de h restes sera composée de nombres tous différents, enfin h restes consécutifs sont toujours différents.

Une première conséquence de cette remarque est la suivante : les seuls termes de la suite qui soient divisibles par m s'obtiennent en multipliant a par un multiple de h ; autrement, *tous les multiples communs à m et à a sont des multiples du plus petit commun multiple ha de ces deux nombres.*

En particulier m doit être un multiple de h, puisque ma est un multiple de m et de a. Soit $m = hd$, soit aussi $ha = mq$; on en déduit $ha = hdq$, d'où $a = dq$: *d est donc un diviseur commun de a et de m, nous allons voir que c'est le plus grand.*

1° Supposons d'abord que a et m soient premiers entre eux ; d ne pourra être égal qu'à l'unité, donc, dans ce cas $h = m$, ce qui s'énonce : *le plus petit commun multiple de deux nombres premiers entre eux est leur produit.* Tout multiple de ces deux nombres est donc un multiple de leur produit, d'où il résulte que *si un nombre divise un produit de deux facteurs et est premier avec l'un d'eux, il divise l'autre.*

Dans ce cas, la période des restes se compose de m termes distincts qui ne peuvent être que les nombres $0, 1, 2, \ldots, m - 1$, rangés dans un certain ordre : on en conclut que si dans l'expression ax, ou dans l'expression $ax + b$, où b est un nombre entier quelconque, on substitue à la place de x, m nombres entiers consécutifs, ou plus généralement un système complet de nombres incongrus (mod. m), on obtiendra un système complet de nombres incongrus (mod. m) ; en substituant dans ax les nombres entiers $1, 2, \ldots, m-1$ à la place de x, on obtient comme restes ces mêmes nombres pris dans un certain ordre ; plus généralement en substituant, à la place de x, $m - 1$ nombres incongrus (mod. m) et dont aucun n'est nul (mod. m) on obtient encore $m - 1$ nombres incongrus (mod. m), dont aucun n'est nul (mod. m).

2° Supposons maintenant que a et m ne soient pas premiers entre eux ; soit δ leur plus grand commun diviseur ; les nombres

$\frac{a}{\delta}$, $\frac{m}{\delta}$ sont premiers entre eux, et l'on observera en passant que cette proposition s'établit directement, sans passer par l'algorithme du plus grand commun diviseur.

Les restes minima que l'on obtient en divisant par $\frac{m}{\delta}$ les termes de la suite

$$0, \quad \frac{a}{\delta}, \quad 2\frac{a}{\delta}, \quad 3\frac{a}{\delta}, \quad \ldots.$$

sont les quotients par δ des restes que l'on obtient en divisant par m les termes de la suite

$$0, \; a, \; 2a, \; 3a, \; \ldots;$$

la périodicité est la même ; d'après ce qu'on vient de dire, la période pour la première suite contient $\frac{m}{\delta}$ restes, qui sont les nombres $0, 1, 2, \ldots, \frac{m}{\delta} - 1$, rangés dans un certain ordre; cette période, pour la seconde suite contiendra aussi $\frac{m}{\delta}$ restes qui seront $0, \delta, 2\delta, \ldots, m - \delta$. Enfin puisque l'on doit avoir $\frac{m}{\delta} = h$, il faut que h soit égal à d, et l'on retrouve en passant le théorème sur la composition du plus petit commun multiple de deux nombres, qui *s'obtient en divisant le produit des deux nombres par leur plus grand commun diviseur.*

On reconnaît aussi, dans ce cas, que si dans l'expression $ax + b$, on remplace x par un système complet de nombres incongrus (mod. m), on n'obtient plus un système complet de nombres incongrus, mais seulement $\frac{m}{\delta}$ restes incongrus.

L'application de ces divers théorèmes aux polygones réguliers étoilés est bien connue.

4. Dans le cas où m est un nombre premier p, chaque nombre non divisible par p est premier à ce nombre : si donc dans l'expression ax où a n'est pas divisible par p on substitue $p - 1$ nombres $x_1, x_2, \ldots, x_{p-1}$ incongrus entre eux et à 0 (mod. p), on obtiendra $p - 1$ nombres congrus à ces mêmes nombres x_1, $x_2, \ldots, x_{p-1}$ rangés dans un autre ordre; le produit des nombres $ax_1, ax_2, \ldots, ax_{p-1}$ est donc congru (mod. p) au produit $x_1 x_2 \ldots . x_{p-1}$, et comme le dernier produit est premier à p,

on en conclut

$$a^{p-1} - 1 \equiv 0 \pmod{p}.$$

C'est le célèbre *théorème de Fermat*, qui joue, dans la théorie des nombres, un rôle essentiel et dont nous rencontrerons incidemment d'autres démonstrations ; observons qu'on en déduit immédiatement la proposition suivante : *quel que soit le nombre entier* a *et le nombre premier* p, *on a*

$$a^p - a \equiv 0 \pmod{p}.$$

II. — Racines des congruences.

5. Nous n'avons considéré, jusqu'ici, que des congruences ne renfermant pas d'indéterminée, des congruences purement arithmétiques, si l'on peut s'exprimer ainsi ; elles correspondent à ce que l'on appelle proprement des *égalités* ; nous allons parler maintenant de celles qui correspondent aux *identités* et aux *équations*. On n'a pas jugé qu'il fût nécessaire de créer des mots distincts pour désigner ces diverses congruences, mais il importe de ne pas les confondre.

On dit que deux polynomes $f(x)$ et $g(x)$ *entiers* par rapport à une variable x (sauf avis contraire, *nous sous-entendrons toujours que les coefficients des polynomes sont entiers*), sont *identiquement congrus* ou plus simplement *congrus suivant un module* m s'il existe un polynome entier en x, $\psi(x)$, tel que l'on ait, quel que soit l'entier x,

$$f(x) = g(x) + m\psi(x).$$

On écrit alors d'une manière abrégée

$$f(x) \equiv g(x) \pmod{m}.$$

Les coefficients des mêmes puissances de x, dans f et dans g, sont évidemment congrus suivant le module m.

D'après cette définition, on a

$$f(x) \equiv 0 \pmod{m}$$

dans le cas et dans le cas seulement où tous les coefficients de $f(x)$ sont divisibles par m.

S'il n'en est pas ainsi, on n'aura pas en général, pour toute valeur entière a de x,

$$f(a) \equiv 0 \pmod{m}.$$

S'il existe un nombre entier a tel que cette congruence soit vérifiée, ce nombre a est dit une *racine* de la congruence

$$f(x) \equiv 0 \qquad (\text{mod. } m).$$

Une congruence peut n'être pas identique et cependant avoir pour racines tous les nombres entiers; si p désigne un nombre premier, c'est ce qui a lieu d'après ce que nous avons vu pour la congruence

$$x^p - x \equiv 0 \qquad (\text{mod. } p).$$

Nous verrons plus tard comment on peut reconnaître, dans le cas d'un module quelconque, si une congruence donnée possède ce caractère exceptionnel (*).

Revenons à la relation

$$f(a) \equiv 0 \qquad (\text{mod. } m),$$

qui exprime que la congruence donnée admet la racine a. Il est clair que si l'on a

$$b \equiv a \qquad (\text{mod. } m),$$

on a aussi

$$f(b) \equiv 0 \qquad (\text{mod. } m),$$

c'est-à-dire que la congruence admet aussi pour racines tous les nombres b congrus au nombre a. *Nous ne regarderons pas ces racines comme distinctes.* Il en résulte qu'une congruence (mod. m) peut avoir au plus m racines distinctes (et même $m-1$ seulement si on ne tient pas compte des racines congrues à zéro). On peut donc toujours résoudre une congruence, c'est-à-dire trouver les racines de cette congruence par un nombre limité d'essais successifs. Mais ces essais sont d'autant plus nombreux que le nombre m est plus grand; d'autre part, on ne connaît pas de méthode générale simple pour résoudre les congruences dont le degré dépasse l'unité. Il y a donc intérêt, pour diminuer le nombre des essais, à réduire s'il est possible la valeur du module m. Nous allons montrer que pour résoudre une congruence, il suffit de résoudre un certain nombre d'autres congruences ayant pour modules des facteurs premiers entrant dans m.

Il faudra de plus résoudre un problème simple qui ne dépend que de congruences du premier degré, et que nous étudierons en détail.

(*) Voir la note à la fin de l'ouvrage.

6. Montrons, en premier lieu, que si l'on a

$$m = pqr,$$

les nombres p, q, r étant *premiers entre eux deux à deux*, on peut ramener la résolution de la congruence

$$(1) \qquad f(x) \equiv 0 \pmod{m}$$

à celle des congruences simultanées :

$$(2) \qquad \begin{cases} f(x) \equiv 0 & \pmod{p}, \\ f(x) \equiv 0 & \pmod{q}, \\ f(x) \equiv 0 & \pmod{r}. \end{cases}$$

En effet, il est clair d'abord que tout nombre x qui satisfait à la congruence (1) satisfait aux trois congruences (2). Réciproquement, si x satisfait aux trois congruences (2), $f(x)$ étant divisible par les trois nombres premiers entre eux deux à deux p, q, r, est divisible par leur produit m, c'est-à-dire que x satisfait à la congruence (1).

Il suffit donc de déterminer les solutions communes aux congruences (2). Pour cela, nous supposerons que nous ayons résolu séparément chacune de ces congruences et nous ferons voir qu'à tout groupe formé d'une racine α de la première, d'une racine β de la seconde et d'une racine γ de la troisième, correspond une racine x de la congruence (1) ; de sorte que si les congruences (2) ont respectivement p', q', r' racines, la congruence (1) en a $p'q'r'$. (Si la première des congruences (2) par exemple était identique ou vérifiée quel que soit x, on aurait $p' = p$).

En effet, il suffit que l'on ait

$$\begin{aligned} x &\equiv \alpha \pmod{p}, \\ x &\equiv \beta \pmod{q}, \\ x &\equiv \gamma \pmod{r}. \end{aligned}$$

Or on conclut immédiatement de là :

$$\begin{aligned} qrx &\equiv qr\alpha \pmod{m}, \\ rpx &\equiv rp\beta \pmod{m}, \\ pqx &\equiv pq\gamma \pmod{m}, \end{aligned}$$

et par suite

$$(qr + rp + pq)x \equiv qr\alpha + rp\beta + pq\gamma \pmod{m}.$$

Nous verrons plus loin que cette congruence du premier degré en x, dans laquelle le coefficient $qr + rp + pq$ de x est premier avec le module $m = pqr$ (puisque p, q, r sont premiers entre

eux deux à deux) a une racine unique et déterminée. Cette racine satisfait d'ailleurs aux conditions exigées ; car on a par exemple

$$(qr + rp + pq)x \equiv qr\alpha + rp\beta + pq\gamma \qquad (\text{mod. } p),$$

d'où, en supprimant de part et d'autre les multiples de p,

$$qrx \equiv qr\alpha \qquad (\text{mod. } p),$$

et enfin, en divisant par qr qui est premier avec le module p,

$$x \equiv \alpha \qquad (\text{mod. } p).$$

Nous avons ainsi montré qu'à tout système de solutions α, β, γ du système (2) correspond une racine x de la congruence (1). Il est clair que la réciproque est vraie et de plus que la correspondance est univoque ; c'est-à dire que si x et x' sont incongrus suivant le module pqr, ils sont incongrus par rapport à l'un au moins des modules p, q, r et réciproquement. Les propositions énoncées sont donc complètement démontrées.

Nous reviendrons d'ailleurs sur la congruence qui détermine x, après avoir traité des congruences du premier degré, pour montrer comment on peut diriger la solution de manière que la plus grande partie du calcul soit indépendante de α, β, γ, c'est-à-dire puisse servir pour toutes les racines.

7. Les résultats acquis résolvent complètement le problème posé dans le cas où m ne renferme pas de facteurs premiers figurant avec une puissance supérieure à la première. Dans le cas contraire, la décomposition la plus complète qui se puisse effectuer de m en un produit de nombres premiers entre eux deux à deux, est la décomposition en un produit de puissances de nombres premiers. Il reste donc à montrer comment on peut ramener la résolution d'une congruence dont le module est une puissance d'un nombre premier, à la résolution de congruences de module premier.

Soit donc

$$(1) \qquad f(x) \equiv 0 \qquad (\text{mod. } p^{\lambda})$$

une congruence dont le module est la puissance d'un nombre premier. Il est clair que toute racine de cette congruence satisfera aussi à la congruence

$$(2) \qquad f(x) \equiv 0 \qquad (\text{mod. } p).$$

Mais la réciproque n'est pas nécessairement exacte. Soit a une ra-

cine de la congruence (2); $a+py$ sera aussi une racine de (2); nous allons chercher à déterminer l'entier y de manière que cette quantité soit également racine de (1).

Nous avons $$f(a+py) = p^\alpha \varphi(y),$$

α étant un nombre au moins égal à 1, $\varphi(y)$ un polynome entier dont tous les coefficients ne sont pas divisibles par p. Si l'on a $\alpha \geqq \lambda$, $a+py$ est racine de la congruence (1) quel que soit l'entier y; à la racine a correspondent ainsi $p^{\lambda-1}$ racines incongrues de la congruence (1).

Si l'on a au contraire $\alpha < \lambda$, la congruence (1) peut s'écrire, en posant $x = a+py$,

$$f(a+py) = p^\alpha \varphi(y) \equiv 0 \qquad (\text{mod. } p^\lambda).$$

On en conclut

$$\varphi(y) \equiv 0 \qquad (\text{mod. } p^{\lambda-\alpha}).$$

La détermination des racines de (1) qui sont congrues au nombre a suivant le module p, est ainsi ramenée à la résolution d'une congruence dans laquelle le module a une moins grande valeur. On voit immédiatement qu'en appliquant la même méthode à cette nouvelle congruence *on n'aura jamais à résoudre que des congruences* (mod. p). On peut vérifier que l'on a ainsi moins d'essais à faire si l'on procède par tâtonnements et de plus, pour ces essais, on opère sur des nombres moins considérables, puisqu'on peut remplacer tous les coefficients d'une congruence (mod. p) par leurs résidus minima absolus, c'est-à-dire par des nombres inférieurs en valeur absolue à $\frac{p}{2}$.

Comme application, considérons la congruence

$$(1) \qquad x^2 \equiv 7 \qquad (\text{mod. } 27).$$

Nous devons d'abord résoudre la congruence

$$x^2 \equiv 7 \qquad (\text{mod. } 3)$$

ou

$$x^2 \equiv 1 \qquad (\text{mod. } 3),$$

qui admet évidemment les deux racines incongrues $+1$ et -1; nous ne considérerons que la racine positive (on obtiendra ensuite en changeant les signes les résultats qui correspondent à la racine négative).

Si nous posons $x = 1+3y$, la congruence proposée devient

$$3(3y^2+2y-2) \equiv 0 \qquad (\text{mod. } 27)$$

ou

(2) $$3y^2 + 2y - 2 \equiv 0 \pmod{9}.$$

Nous devons d'abord résoudre la congruence

$$3y^2 + 2y - 2 \equiv 0 \pmod{3},$$

qui donne

$$y \equiv 1 \pmod{3}$$

et nous conduit à poser $y = 1 + 3z$.

La congruence (2) devient alors

$$3[(1 + 3z)^2 + 2z] \equiv 0 \pmod{9}$$

ou

$$(1 + 3z)^2 + 2z \equiv 0 \pmod{3}$$

$$1 + 2z \equiv 0 \pmod{3},$$

d'où

$$z \equiv 1 \pmod{3}.$$

On a donc $y = 4$ et $x = 13$; la congruence (1) admet les deux racines $+13$ et -13 ou, si l'on veut, 13 et 14. La congruence proposée est d'ailleurs l'une de celles pour lesquelles il existe des méthodes générales de résolution.

8. Avant de passer à l'étude générale des congruences de degré quelconque et particulièrement des congruences de module premier, étude qui fera l'objet du chapitre suivant, nous allons traiter en détail des *congruences du premier degré*. Il est en effet nécessaire de les traiter dans le cas d'un module quelconque et de plus leur étude nous conduira à nous occuper de diverses questions intéressantes en elles-mêmes.

Considérons d'abord le cas d'un module premier p. La congruence du premier degré a la forme

$$ax \equiv b \pmod{p}.$$

Elle est *identique*, si a et b sont tous deux congrus à zéro (mod. p), *impossible* si a est congru à zéro sans que b le soit. Ces résultats qui s'aperçoivent immédiatement sont absolument pareils à ceux que l'on obtient dans l'étude des équations du premier degré.

Dans le cas où a n'est pas congru à zéro, il résulte de remarques déjà faites que si l'on donne à x, p valeurs incongrues, le premier membre prendra p valeurs incongrues, dont par conséquent une et une seule sera congrue à b. La congruence a donc *une racine et une seule ;* le théorème de Fermat permet d'avoir immédiatement

son expression : si l'on multiplie les deux membres de la congruence par a^{p-2}, on obtient

$$a^{p-1}x \equiv ba^{p-2} \pmod{p};$$

d'autre part, a étant premier avec p,

$$a^{p-1} \equiv 1 \pmod{p}.$$

On a donc enfin

$$x \equiv ba^{p-2} \pmod{p}.$$

Gauss convient de représenter la racine de la congruence du premier degré par $\frac{b}{a}$ (mod. p), c'est-à-dire d'écrire

$$x \equiv \frac{b}{a} \pmod{p}.$$

Les expressions telles que $\frac{b}{a}$ (mod. p) ne sont pas des fractions, mais des nombres entiers ; *il est cependant facile de vérifier qu'elles sont soumises aux mêmes règles de calcul que les fractions ordinaires.* Il importe seulement de remarquer qu'on doit exclure du calcul, comme n'ayant pas de sens, celles dont le dénominateur est *congru à zéro* et qu'on ne doit jamais multiplier les deux termes par un nombre *congru à zéro*. Dès lors il est facile de vérifier, par exemple, que si l'on a

$$x \equiv \frac{a}{b} \pmod{p},$$

$$y \equiv \frac{c}{d} \pmod{p},$$

il en résulte

$$x + y \equiv \frac{ad + bc}{bd} \pmod{p},$$

$$xy \equiv \frac{ac}{bd} \pmod{p},$$

$$\frac{x}{y} \equiv \frac{ad}{bc} \pmod{p},$$

en supposant, bien entendu, qu'aucun des dénominateurs n'est congru à zéro. *Ces égalités sont des égalités entre nombres entiers ;* la dernière, par exemple, exprime que x et y étant les racines des congruences

$$bx - a \equiv 0 \pmod{p},$$

$$dy - c \equiv 0 \pmod{p},$$

les congruences

$$yX - x \equiv 0 \pmod{p},$$

$$bcX - ad \equiv 0 \pmod{p}$$

sont équivalentes. C'est ce qu'il est aisé de vérifier directement, b, c, d étant supposés incongrus à zéro.

Les remarques précédentes nous conduisent naturellement à considérer la racine x de la congruence

$$ax \equiv 1 \pmod{p},$$

c'est-à-dire

$$x \equiv \frac{1}{a} \pmod{p}.$$

Sa connaissance est manifestement utile dans le calcul des racines des congruences de la forme

$$ax \equiv b \pmod{p}$$

ou

$$x \equiv \frac{b}{a} \pmod{p}.$$

Il est clair en effet que si l'on a

$$a' \equiv \frac{1}{a},$$

il en résulte

$$\frac{b}{a} \equiv a'b.$$

Le nombre a' est dit le *nombre associé* de a. Il est clair que la correspondance entre a et a' est réciproque. D'ailleurs a ne peut être égal à a' que si leur valeur commune est 1 ou $p-1$, car si $a'=a$, on a

$$a^2-1=(a-1)(a+1)\equiv 0 \pmod{p},$$

et p étant premier divise $a-1$ ou $a+1$.

Les nombres $2, 3, \ldots\ldots, p-2$ sont donc associés deux à deux; le produit de deux nombres associés étant congru à 1, il en résulte

$$2.3\ldots\ldots(p-2)\equiv 1 \pmod{p},$$

d'où

$$1.2.3\ldots\ldots(p-2)(p-1)\equiv p-1\equiv -1 \pmod{p},$$

ou enfin

$$1.2.3\ldots\ldots(p-1)+1\equiv 0 \pmod{p}.$$

Cette égalité constitue le *théorème de Wilson*, remarquable par le fait qu'il exprime une propriété *caractéristique* des nombres premiers. En effet, si p n'est pas premier, on voit facilement que le produit $1.2.3\ldots\ldots(p-1)$ est divisible par p.

9. Indiquons maintenant une méthode de résolution des congruences du premier degré *de module composé*, méthode qui s'applique d'ailleurs aussi dans le cas d'un module premier.

Soit

$$ax \equiv b \pmod{m}$$

une congruence ; on peut, en désignant par y un entier indéterminé, la remplacer par l'équation

$$ax + my = b.$$

On est ainsi ramené à un problème traité dans les éléments sous le nom d'*analyse indéterminée* du premier degré.

On sait que si a et m sont premiers entre eux, toutes les valeurs de x qui satisfont à cette équation sont de la forme

$$x = x_0 + mt,$$

c'est-à-dire

$$x \equiv x_0 \pmod{m}.$$

La congruence proposée admet donc dans ce cas une solution unique ; pour la trouver, on réduit $\frac{a}{m}$ en fraction continue, et en désignant par $\frac{\alpha}{\mu}$ l'avant-dernière réduite, on a, la dernière réduite étant précisément $\frac{a}{m}$,

$$a\mu - m\alpha = \pm 1,$$

et par suite

$$a(\pm b\mu) - m(\pm b\alpha) = b.$$

Dans le cas où a et m ont un diviseur commun δ, le problème est impossible si δ ne divise pas b. Si δ divise b, on est ramené à l'équation

$$\frac{a}{\delta}x + \frac{m}{\delta}y = \frac{b}{\delta},$$

c'est-à-dire, si l'on veut, à la congruence

$$\frac{a}{\delta}x \equiv \frac{b}{\delta} \quad \left(\text{mod.}\ \frac{m}{\delta}\right).$$

On a donc à résoudre le même problème ; cette dernière congruence a une solution unique x_0, mais la congruence proposée admet pour solutions distinctes tous les nombres congrus à x_0 suivant le module $\frac{m}{\delta}$ et incongrus suivant le module m ; elle a donc δ solutions.

On voit que l'on peut employer pour les modules composés la notation de Gauss que nous avons indiquée pour les modules premiers, mais on doit exclure tous les dénominateurs non premiers

avec le module. La solution que nous venons d'indiquer revient d'ailleurs à chercher d'abord la valeur du symbole $\frac{1}{a}$ (mod. m), c'est-à-dire à déterminer l'associé a' du nombre a. Dans le calcul fait plus haut on a

$$a' = \pm \mu.$$

Nous pouvons maintenant traiter d'une manière complète le problème qui s'était offert à propos des congruences quelconques de module composé et qu'on peut formuler ainsi : p, q, r étant des nombre premiers entre eux deux à deux, trouver un nombre x qui satisfasse aux congruences

$$x \equiv \alpha \qquad (\text{mod. } p),$$
$$x \equiv \beta \qquad (\text{mod. } q),$$
$$x \equiv \gamma \qquad (\text{mod. } r).$$

Nous avons trouvé que x est déterminé par la congruence unique

$$(qr + rp + pq)x \equiv qr\alpha + rp\beta + pq\gamma \qquad (\text{mod. } m = pqr).$$

Or, d'après les hypothèses faites, $qr + rp + pq$ est premier avec m; déterminons son associé, c'est-à-dire calculons un nombre m' par la congruence

$$m'(qr + rp + pq) \equiv 1 \qquad (\text{mod. } m).$$

On aura

$$x \equiv qr\alpha m' + rp\beta m' + pq\gamma m' \qquad (\text{mod. } m).$$

On voit que la détermination de m' est complètement indépendante de α, β, γ, comme nous l'avions annoncé plus haut.

On peut mettre la formule obtenue sous une autre forme. Si nous déterminons en effet p', q', r' par les congruences

$$p'(qr + rp + pq) \equiv 1 \qquad (\text{mod. } p),$$
$$q'(qr + rp + pq) \equiv 1 \qquad (\text{mod. } q),$$
$$r'(qr + rp + pq) \equiv 1 \qquad (\text{mod. } r),$$

qui peuvent s'écrire, plus simplement,

$$p'qr \equiv 1 \qquad (\text{mod. } p),$$
$$q'rp \equiv 1 \qquad (\text{mod. } q),$$
$$r'pq \equiv 1 \qquad (\text{mod. } r),$$

on aura

$$m' = p' + hp, \qquad m' = q' + kq, \qquad m' = r' + lr,$$

h, k, l étant des entiers inconnus; il en résulte

$$x \equiv qr\alpha p' + rp\beta q' + pq\gamma r' + (h\alpha + k\beta + l\gamma)pqr \quad (\text{mod. } m),$$

ou plus simplement

$$x \equiv p'qr\alpha + q'rp\beta + r'pq\gamma \qquad (\text{mod. } m).$$

On obtient aisément cette valeur de x en remarquant que si l'on pose

$$\xi \equiv \alpha, \quad \eta \equiv 0, \quad \zeta \equiv 0, \qquad (\text{mod. } p),$$
$$\xi \equiv 0, \quad \eta \equiv \beta, \quad \zeta \equiv 0, \qquad (\text{mod. } q),$$
$$\xi \equiv 0, \quad \eta \equiv 0, \quad \zeta \equiv \gamma, \qquad (\text{mod. } r),$$

on a

$$x \equiv \xi + \eta + \zeta \qquad (\text{mod. } m).$$

Or, on trouve immédiatement

$$\xi \equiv p'qr\alpha \qquad (\text{mod. } m),$$

et de même les valeurs de η et ζ.

Il est à peine utile de faire observer que rien ne serait changé à la méthode si au lieu de trois nombres p, q, r il y en avait un plus grand nombre.

10. Revenons à l'*étude des nombres associés dans le cas d'un module composé*; nous avons dit que a et a' sont associés lorsque l'on a

$$aa' \equiv 1 \qquad (\text{mod. } m).$$

Les nombres qui sont premiers avec le module sont les seuls qui possèdent des associés; deux nombres associés sont égaux si en désignant par a leur valeur commune, on a la congruence

$$a^2 \equiv 1 \qquad (\text{mod. } m).$$

Si cette congruence admet la racine a, elle admet la racine $m - a$ et ces deux racines sont distinctes, car si elles ne l'étaient pas leur produit serait congru à 1; or on a

$$a(m - a) \equiv -a^2 \equiv -1 \qquad (\text{mod. } m)$$

et nous supposons m supérieur à 2.

On conclut très facilement de ce qui précède que si l'on désigne par $\psi(m)$ le nombre des racines de la congruence

$$x^2 \equiv 1 \qquad (\text{mod. } m),$$

et par P le produit de tous les nombres premiers avec m et non supérieurs à m, on a

$$\text{P} \equiv (-1)^{\frac{1}{2}\psi(m)} \qquad (\text{mod. } m).$$

Cette égalité constitue le *théorème de Wilson généralisé*. On peut chercher directement l'expression de $\psi(m)$ (voir à ce sujet : Serret,

Algèbre supérieure, § 292) ; nous déduirons sa valeur de la théorie générale des congruences binomes qui sera faite plus loin. Nous verrons que l'on a

$$\psi(m) = 2^{\mu+\eta},$$

μ étant le nombre des facteurs premiers impairs *distincts* de m, et η étant égal à *zéro* si m n'est pas divisible par 4, à *un* si m est divisible par 4 et non par 8, à *deux* si m est divisible par 8.

Il en résulte que *l'on a*

$$P \equiv -1 \qquad (\text{mod. } m)$$

lorsque m est égal à une puissance d'un nombre premier impair, égal au double d'une telle puissance ou égal à 4, et au contraire

$$P \equiv +1 \qquad (\text{mod. } m)$$

dans tous les autres cas.

On voit que *les nombres inférieurs à m et premiers avec m* jouent dans cet énoncé le même rôle que les nombres inférieurs au module, dans le cas du module premier. On peut aller plus loin dans cet ordre d'idées et remarquer que l'ensemble de ces nombres jouit de certaines propriétés du système complet des restes dans le cas du module premier.

Par exemple, si on multiplie tous les nombres de cet ensemble par un nombre a premier avec m (c'est-à-dire appartenant aussi à cet ensemble), on obtient comme produits des nombres tous incongrus et de plus premiers avec m. Ce sont donc, dans un certain ordre, les nombres de l'ensemble considéré. On voit que ces raisonnements sont tout pareils à ceux par lesquels on établit le théorème de Fermat ; en continuant à raisonner d'une manière analogue, on établit sans peine la formule

$$a^{\varphi(m)} \equiv 1 \qquad (\text{mod. } m),$$

dans laquelle a désigne un nombre quelconque premier avec m et $\varphi(m)$ *le nombre des nombres premiers avec m et non supérieurs à m.*

La propriété exprimée par cette formule est ce qu'on appelle le *théorème de Fermat généralisé.* Il est, de même que le théorème de Wilson généralisé, beaucoup moins intéressant et moins important que la proposition simple. Il ne fournit pas, en effet, de congruence qui soit vérifiée pour toute valeur de la variable, sans être une identité, tandis que nous verrons que c'est, au fond, ce qui constitue l'importance considérable du théorème de Fermat. Celui-ci

est réellement dans la nature des choses et, dans les chapitres qui vont suivre, il s'en présentera, incidemment, plusieurs démonstrations nouvelles.

III. — La fonction $\varphi(m)$.

11. Nous avons néanmoins tenu à parler du théorème de Fermat généralisé, qui a d'ailleurs une certaine importance dans la théorie générale des congruences binomes, car il nous donne le premier exemple de l'introduction dans une formule d'une fonction arithmétique très importante, la fonction $\varphi(m)$.

Lorsque m est plus grand que 1, on peut dire que $\varphi(m)$ est le nombre des nombres premiers à m et plus petits que lui; c'est pour pouvoir supposer

$$\varphi(1) = 1,$$

que l'on dit « non supérieurs à m ».

La fonction $\varphi(m)$ va nous arrêter quelque temps, et les considérations antérieures nous en fourniront les propriétés essentielles.

La plus simple est exprimée par l'égalité

$$\varphi(ab) = \varphi(a) \times \varphi(b),$$

où a, b sont deux entiers positifs premiers entre eux, égalité que nous allons établir.

Elle est évidente si l'un des nombres a, b est égal à un; nous supposerons donc les deux nombres plus grands que un. Dès lors si l'on considère un nombre entier positif premier à ab et plus petit que ab, on pourra le mettre sous la forme $ax + y$, en désignant par x le quotient de sa division par a et par y le reste de ces deux nombres, x est inférieur à b, y est inférieur à a et premier avec a. Inversement, si x est inférieur à b et y inférieur à a et premier avec a, $ax + y$ est inférieur à ab et premier à a. Le nombre y peut prendre $\varphi(a)$ valeurs; considérons l'une d'elles et voyons combien elle fournit pour $ax + y$ de valeurs premières à b et par suite à ab; si on donne dans $ax + y$ les valeurs $0, 1, 2, \ldots, b - 1$ à x, on obtiendra un système complet de nombres incongrus (mod. b); parmi ces derniers nombres, il y a $\varphi(b)$ nombres premiers à b; parmi les nombres que l'on déduit de $ax + y$ en remplaçant x par $0, 1, 2, \ldots, b - 1$, il y aura

donc aussi $\varphi(b)$ nombres premiers à ab ; on voit qu'il y aura $\varphi(a) \times \varphi(b)$ nombres premiers à ab et inférieurs à ab ; l'égalité est démontrée.

On reconnait de suite que si m est une puissance p^α d'un nombre premier p, on a

$$\varphi(m) = p^{\alpha-1}(p-1) = m\left(1 - \frac{1}{p}\right);$$

il en résulte que si l'on suppose m décomposé en ses facteurs premiers,

$$m = p^\alpha q^\beta r^\gamma \ldots\ldots$$

on aura

$$\varphi(m) = \varphi(p^\alpha)\varphi(q^\beta)\varphi(r^\gamma)\ldots = m\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right)\left(1 - \frac{1}{r}\right)\ldots$$

Une autre propriété capitale de la fonction φ va résulter encore du même genre de considérations. Si l'on envisage la suite

$$0,\ a,\ 2a,\ \ldots,$$

et la suite des restes minima que l'on obtient en en divisant les termes par m, la période des restes comprend m termes ou $\frac{m}{\delta}$ termes suivant que m est premier à a ou admet avec a le plus grand commun diviseur δ. Ce nombre de termes est dans tous les cas un diviseur de m.

Inversement, si d est un diviseur de m, il existe des nombres a tels que la période des restes ait d termes ; il faut et il suffit en effet que le plus grand commun diviseur de a et de m soit $\delta = \frac{m}{d}$, c'est-à-dire que les quotients de m et de a par $\frac{m}{d}$ soient premiers entre eux, c'est-à-dire encore que d et $\frac{ad}{m}$ soient premiers entre eux ; on devra donc, pour cela, prendre a de la forme $\frac{m}{d}k$, k étant premier à d.

Prenons successivement pour a les valeurs $0, 1, 2, \ldots, m-1$; la valeur 0 fournira des restes tous nuls, c'est d'ailleurs la seule dans ce cas ; la période des restes ne comprendra qu'un terme. Les nombres qui fourniront une période de d termes seront de la forme $\frac{m}{d}k$, k étant premier à d et inférieur à d, afin que $\frac{m}{d}k$ soit inférieur

à m, il y en aura $\varphi(d)$; les nombres qui fourniront une période de m restes seront les nombres inférieurs à m et premiers à m.

En résumé, on a

$$m = 1 + \varphi(d) + \varphi(d') + \ldots + \varphi(m),$$

en désignant par d, d', ... les diviseurs de m autres que *un* et m, ou

$$m = \Sigma\varphi(d),$$

en supposant que d représente successivement tous les diviseurs de m, y compris m et un.

12. On n'aurait aucune peine à vérifier cette égalité, au moyen de l'expression connue des diviseurs d d'un nombre m décomposé en ses facteurs premiers et de l'expression trouvée antérieurement pour $\varphi(m)$. Tout au contraire, nous voulons déduire de cette formule l'expression de $\varphi(m)$, par une méthode assurément plus longue et plus difficile, mais qui comporte l'établissement d'une formule importante.

Nous démontrerons d'abord le lemme suivant. Parmi les diviseurs d'un nombre m plus grand que un, ne considérons que ceux dont les facteurs premiers sont tous différents : *le nombre de ceux qui contiennent un nombre impair de facteurs premiers surpasse d'une unité le nombre de ceux qui contiennent un nombre pair de facteurs premiers.*

Ceci n'est autre chose que cette propriété bien connue : *le nombre des combinaisons formées avec n objets en prenant un nombre impair de ces objets, surpasse d'une unité le nombre des combinaisons formées avec les mêmes objets en en prenant un nombre pair.*

Si donc on pose

$$\varepsilon_1 = 1,$$

puis, en supposant que m soit un entier plus grand que 1,

$$\varepsilon_m = 0$$

quand le nombre entier positif m contient au moins un facteur premier élevé à une puissance plus grande que un, et enfin

$$\varepsilon_m = (-1)^n$$

quand m ne contient que des facteurs premiers différents, en nombre égal à n, on aura

$$\Sigma\varepsilon_d = 0,$$

la sommation étant étendue à tous les diviseurs d d'un nombre quelconque plus grand que un, y compris ce nombre et l'*unité* (*).

Observons en passant, avec Kronecker, que cette égalité contient une démonstration de la formule d'Euler

$$\left[\sum_{n=1}^{n=\infty} \frac{1}{n^z}\right]\left[\prod_{(p)}\left(1-\frac{1}{p^z}\right)\right] = 1,$$

où, dans le produit infini, p doit prendre les valeurs de tous les nombres premiers autres que 1, et où z est un nombre quelconque réel ou imaginaire dont la partie réelle est toutefois plus grande que un, afin que la série et le produit infini soient absolument convergents. En effet, en développant le produit infini, on trouve évidemment

$$\prod_{(p)}\left(1-\frac{1}{p^z}\right) = \sum_{m=1}^{m=\infty} \frac{\varepsilon_m}{m^z}$$

et d'ailleurs le produit des deux séries

$$\sum_{n=1}^{n=\infty} \frac{1}{n^z} \sum_{m=1}^{m=\infty} \frac{\varepsilon_m}{m^z} = \sum_{m,n} \frac{\varepsilon_m}{(mn)^z}$$

est égal à un, car si a est un entier quelconque plus grand que un, le terme $\frac{1}{a^z}$ y figurera avec un coefficient égal à la somme $\Sigma\varepsilon_d$ étendue à tous les diviseurs du nombre a.

13. Considérons maintenant un nombre entier positif quelconque m, désignons par $f(x)$ une fonction numérique définie pour toutes les valeurs entières et positives de x, et définissons la fonction numérique $\mathrm{F}(m)$ par la formule

$$(1) \qquad \mathrm{F}(m) = \Sigma f(d),$$

où, dans le second membre, la sommation est étendue à tous les diviseurs d de m, y compris m et l'unité.

Nous allons démontrer que l'on a inversement

(*) En effet l'unité n'intervient pas au nombre des diviseurs de m dans le lemme énoncé plus haut, car elle ne renferme aucun facteur premier; en convenant de considérer l'unité comme renfermant *zéro* facteur premier, c'est-à-dire un nombre pair, on remplacerait dans l'énoncé du lemme : *surpasse d'une unité* par : *est égal à*.

$$(2) \qquad f(m) = \Sigma \varepsilon_d F\left(\frac{m}{d}\right);$$

si l'on remplace en effet $F\left(\frac{m}{d}\right)$ par sa définition, dans le second membre, il deviendra

$$\Sigma \varepsilon_d [\Sigma f(d')],$$

où le second signe Σ se rapporte à tous les diviseurs d' de $\frac{m}{d}$; si l'on réduit les termes semblables, on voit que $f(d')$ sera multiplié par $\Sigma \varepsilon_\delta$, où la sommation s'étend à tous les diviseurs δ de m tels que $\frac{m}{\delta}$ soit divisible par d', ou que $\frac{m}{d'}$ soit divisible par δ, c'est-à-dire à tous les diviseurs de $\frac{m}{d'}$; on aura donc $\Sigma \varepsilon_\delta = 0$ si d' n'est pas égal à m, $\Sigma \varepsilon_\delta = \varepsilon_1 = 1$ si d' est égal à m. On a donc bien

$$\Sigma \varepsilon_d [\Sigma f(d')] = f(m).$$

Réciproquement, si la fonction numérique $f(m)$ est définie par l'égalité (2), la fonction $F(m)$ satisfera à l'égalité (1) ; la démonstration est la même.

Si l'on se reporte à la définition du symbole ε_m et si l'on suppose que le nombre m soit décomposé en ses facteurs premiers,

$$m = p^\alpha q^\beta r^\gamma \ldots u^\lambda,$$

$p, q, r, \ldots, u$ étant différents, on voit que l'égalité

$$F(m) = \Sigma f(d)$$

équivaut à la suivante :

$$f(m) = F(m) - \Sigma F\left(\frac{m}{p}\right) + \Sigma F\left(\frac{m}{pq}\right) - \Sigma F\left(\frac{m}{pqr}\right) - \cdots,$$

où $\Sigma F\left(\frac{m}{p}\right)$ est mis pour la somme $F\left(\frac{m}{p}\right) + F\left(\frac{m}{q}\right) + F\left(\frac{m}{r}\right) + \cdots$, $\Sigma F\left(\frac{m}{pq}\right)$ pour la somme $F\left(\frac{m}{pq}\right) + F\left(\frac{m}{pr}\right) + F\left(\frac{m}{qr}\right) + \cdots$, etc.

En particulier l'égalité

$$m = \Sigma \varphi(d)$$

équivaut à celle-ci :

$$\varphi(m) = m - \Sigma \frac{m}{p} + \Sigma \frac{m}{pq} - \Sigma \frac{m}{pqr} + \cdots$$

$$= m\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right)\left(1 - \frac{1}{r}\right)\cdots,$$

et l'on voit que *l'égalité*

$$m = \Sigma \varphi(d)$$

définit entièrement la fonction numérique $\varphi(m)$.

Observons encore, relativement à la formule

$$\varphi(m) = m - \Sigma\frac{m}{p} + \Sigma\frac{m}{pq} - \Sigma\frac{m}{pqr} + \cdots,$$

qu'elle exprime simplement ce fait évident que, si l'on supprime des nombres $1, 2, \ldots, m$ les nombres qui ont un diviseur commun avec m, il ne restera que les nombres premiers à m.

Imaginons en effet les nombres $1, 2, \ldots, m$ écrits dans un tableau

(1) $$+1, +2, \ldots, +m$$

et tous affectés du signe $+$; adjoignons à ce tableau celui des nombres

(2) $$\begin{array}{l} -p, \ -2p, \ -3p, \ \ldots, \ -\frac{m}{p}p, \\ -q, \ -2q, \ -3q, \ \ldots, \ -\frac{m}{q}q, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots \end{array}$$

dont chaque ligne est obtenue en plaçant le signe $-$ devant un des multiples de l'un des nombres $p, q, r, \ldots$ qui sont au plus égaux à m ; adjoignons-y encore le tableau

(3) $$\begin{array}{l} +pq, \ +2pq, \ +3pq, \ \ldots, \ +\frac{m}{pq}pq, \\ +pr, \ +2pr, \ +3pr, \ \ldots, \ +\frac{m}{pr}pr, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots \end{array}$$

dont chaque ligne est obtenue en mettant le signe $+$ devant un multiple de l'un des produits différents obtenus en prenant *deux* des nombres $p, q, r, \ldots$, multiple qui doit être au plus égal à m ; adjoignons-y encore le tableau

(4) $$\begin{array}{l} -pqr, \ -2pqr, \ -3pqr, \ \ldots, \ -\frac{m}{pqr}pqr, \\ -pqs, \ -2pqs, \ -3pqs, \ \ldots, \ -\frac{m}{pqs}pqs, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots \end{array}$$

et ainsi de suite, en alternant les signes à chaque tableau, jusqu'à ce qu'on ait épuisé toutes les combinaisons une à une, deux à deux, ..., n à n des n lettres $p, q, r, \ldots, u$. Dans le tableau final (T) les nombres premiers à m ne figureront qu'une fois, dans (1), avec le signe $+$; considérons maintenant un nombre A non premier avec

m, et non supérieur à m, qui ait avec m exactement k facteurs premiers distincts communs, savoir $p, q, r, \ldots, t$: A figurera une fois dans (1) avec le signe $+$; il figurera dans les p lignes de (2), à savoir les lignes qui contiennent les multiples de p, de $q, \ldots,$ ou de t; A figurera C_k^2 fois dans (3), à savoir dans les lignes qui contiennent les multiples du produit de deux des nombres $p, q, \ldots, t$; etc... En résumé, si dans le tableau final, on réduisait les termes semblables comme dans une addition, A figurerait avec le coefficient

$$1 - C_k^1 + C_k^2 - C_k^3 + \ldots = 0.$$

Il suffit maintenant d'observer que les tableaux partiels (1), (2), (3), ... contiennent respectivement m, $\sum \frac{m}{p}$, $\sum \frac{m}{pq}$, ... termes pour obtenir l'expression développée de $\varphi(m)$.

14. Cette démonstration nous a appris quelque chose de nouveau, en nous montrant *comment on peut constituer l'ensemble des nombres* 1, 2, .., m *qui ont un diviseur commun avec* m ; nous allons l'appliquer immédiatement, ainsi que le théorème du paragraphe précédent, à l'équation binome

$$x^m - 1 = 0,$$

en conservant les mêmes notations pour le nombre m supposé décomposé en ses facteurs premiers.

En posant

$$x_k = e^{\frac{2k\pi i}{m}},$$

on a

$$x^m - 1 = \prod_{k=1}^{k=m} (x - x_k);$$

et en observant que l'on a, par exemple,

$$\prod_{k=1}^{k=\frac{m}{p}} (x - x_{kp}) = x^{\frac{m}{p}} - 1,$$

la démonstration précédente montre clairement que l'expression

$$\theta_m(x) = (x^m - 1)\frac{\prod\left(x^{\frac{m}{pq}} - 1\right)\prod\left(x^{\frac{m}{pqrs}} - 1\right)\ldots}{\prod\left(x^{\frac{m}{p}} - 1\right)\prod\left(x^{\frac{m}{pqr}} - 1\right)\ldots},$$

où $\prod\left(x^{\frac{m}{p}}-1\right)$ est le produit des facteurs $x^{\frac{m}{p}}-1$, $x^{\frac{m}{q}}-1$, ...,
où $\prod\left(x^{\frac{m}{pq}}-1\right)$ est le produit des facteurs $x^{\frac{m}{pq}}-1$, $x^{\frac{m}{pr}}-1$, ...,
etc..., n'est autre chose que le produit des facteurs $x-x_k$ pour lesquels k est premier à m.

Si l'on pose maintenant

$$F(m)=\log(x^m-1),$$
$$f(m)=\log\theta(x),$$

on aura

$$f(m)=\sum\varepsilon_d F\left(\frac{m}{d}\right),$$

la sommation étant étendue à tous les diviseurs de d et le symbole ε_d ayant le sens déjà défini ; on en conclut

$$F(m)=\sum f(d)$$

et par suite

$$x^m-1=\prod\theta_d(x),$$

chacun des facteurs $\theta_d(x)$ ne contenant plus que les facteurs premiers relatifs aux racines primitives de l'équation x^d-1.

On a par exemple

$$x^{60}-1=\theta_{60}\,\theta_{30}\,\theta_{20}\,\theta_{15}\,\theta_{12}\,\theta_{10}\,\theta_{6}\,\theta_{5}\,\theta_{4}\,\theta_{3}\,\theta_{2}\,\theta_{1}\,;$$

en posant

$$\theta_{60}=x^{16}+x^{14}-x^{10}-x^8-x^6+x^2+1,$$
$$\theta_{30}=x^8+x^7-x^5-x^4-x^3+x+1,$$
$$\theta_{20}=x^8-x^6+x^4-x^2+1,$$
$$\theta_{15}=x^8-x^7+x^5-x^4+x^3-x+1,$$
$$\theta_{12}=x^4-x^2+1,$$
$$\theta_{10}=x^4-x^3+x^2-x+1,$$
$$\theta_{6}=x^2-x+1,$$
$$\theta_{5}=x^4+x^3+x^2+x+1,$$
$$\theta_{4}=x^2+1,$$
$$\theta_{3}=x^2+x+1,$$
$$\theta_{2}=x+1,$$
$$\theta_{1}=x-1.$$

CHAPITRE II

DES CONGRUENCES DE MODULE PREMIER

I. — Divisibilité suivant un module premier.

15. Nous allons aborder maintenant la théorie générale des congruences, en insistant tout particulièrement sur le cas du module premier. Nous avons vu en effet qu'on pouvait, en pratique, ramener tous les cas à celui-là ; ce n'est d'ailleurs pas une raison suffisante pour écarter complètement l'étude théorique du cas général, car, lorsqu'on résout un problème en le décomposant en d'autres problèmes plus aisés à aborder, la vraie nature de la solution échappe souvent. Mais, en fait, dans ce qu'on peut appeler la théorie générale des congruences, par analogie avec ce qu'on nomme théorie générale des équations, l'étude des modules premiers est de beaucoup la plus intéressante, précisément parce que l'analogie avec la théorie des équations y est très grande. Un exemple fort simple le fera bien comprendre et en même temps fera pressentir les difficultés qu'on rencontrerait dans une étude du cas des modules composés.

Considérons la congruence

$$(x-1)(x-3) \equiv 0 \pmod{7}.$$

D'après une remarque déjà faite, le produit $(x-1)(x-3)$ ne peut être *nul* (mod. 7) que si l'un de ses facteurs est *nul* (mod. 7) [nous disons, pour abréger le langage et surtout pour le rendre plus expressif : *nul* (mod. 7), au lieu de : *congru à zéro suivant le module* 7 ou *divisible par* 7]. La congruence proposée a donc seulement *deux* racines, qui sont

$$x \equiv 1 \pmod{7},$$
$$x \equiv 3 \pmod{7}.$$

Considérons maintenant la congruence

$$(x-1)(x-3) \equiv 0 \pmod{12}.$$

On vérifie sans peine qu'elle admet les *quatre* racines

$$\begin{cases} x \equiv 1 \\ x \equiv 3 \\ x \equiv 7 \\ x \equiv 9 \end{cases} \pmod{12}.$$

De même, la congruence

$$(x-1)(x-4) \equiv 0 \pmod{9}$$

admet les *trois* racines

$$\begin{cases} x \equiv 1 \\ x \equiv 4 \\ x \equiv 7 \end{cases} \pmod{9}.$$

On voit que, dans le cas du module premier, l'analogie de la congruence considérée avec une équation du second degré ayant ses deux racines réelles, est aussi parfaite que possible ; il en est tout autrement dans le cas du module composé. Aussi, *allons-nous nous occuper exclusivement des modules premiers.*

16. L'exemple que nous venons de donner, et aussi l'analogie *pressentie et cherchée* avec la théorie des équations, conduisent à penser que la théorie générale des congruences a pour base une théorie de la divisibilité analogue à celle qui est faite en Algèbre pour les polynomes. C'est en effet d'une étude de la divisibilité, faite au point de vue spécial des *congruences*, que nous allons nous occuper tout d'abord ; c'est ce que nous appellerons la *théorie de la divisibilité suivant un module premier.*

Si l'on voulait faire une théorie de la divisibilité *des nombres entiers* par rapport à un module premier p, elle serait tout de suite terminée : tout d'abord, si l'on traite les nombres congrus (mod. p) comme égaux, il n'y a plus qu'un nombre fini de nombres distincts, à savoir les nombres $0, 1, 2, \ldots, p-1$. Le théorème : un produit de deux facteurs ne peut être nul (mod. p), c'est-à-dire divisible par p, que si l'un des facteurs est nul (mod. p) subsiste, ainsi que ses conséquences ; mais tout nombre doit être regardé comme divisible (mod. p) par un nombre quelconque non nul (mod. p), puisque si a n'est pas nul (mod. p), la congruence

$$ax \equiv b \pmod{p}$$

admet une solution, en sorte qu'il n'y a rien de pareil aux nombres premiers.

Les nombres distincts et différents de 0 (mod. p), c'est-à-dire les nombres $1, 2, \ldots, p-1$ forment un *groupe fini*, c'est-à-dire que le produit de deux quelconques d'entre eux est congru à un de ces nombres (mod. p), et c'est à cette proposition jointe à ce fait qu'un produit de deux facteurs ne peut être nul que si l'un des facteurs est nul, que se rattache la démonstration du théorème de Fermat.

Au contraire la théorie de la divisibilité *des polynomes* par rapport à un module premier p va nous fournir les analogues des théories du plus grand commun diviseur, des nombres premiers, etc...

Rappelons que, sauf indication expresse du contraire, tous les polynomes considérés sont à coefficients entiers. Comme nous l'avons déjà expliqué, nous dirons qu'un polynome $f(x)$ est identiquement nul (mod. p) lorsque tous ses coefficients sont divisibles par p; et qu'un polynome $f(x)$ admet la racine $x \equiv \alpha$ (mod. p) si $f(\alpha)$ est nul (mod. p), c'est-à-dire est divisible par p.

La proposition fondamentale qu'un produit de deux nombres ne peut être nul (mod. p) que si un des facteurs est nul s'étend sans peine aux polynomes : *Le produit de deux polynomes* $f(x)$ *et* $g(x)$ *ne peut être identiquement nul* (mod. p) *que si un des facteurs est identiquement nul* (mod. p).

En effet, si f et g ne sont pas identiquement nuls (mod. p), ordonnons-les par rapport aux puissances décroissantes de x et désignons par F et G les premiers coefficients qui ne soient pas nuls (mod. p); le terme du degré le plus élevé dans le produit, après suppression des termes à coefficient nul (mod. p), aura un coefficient congru à FG (mod. p) et par suite non nul (mod. p). Le produit n'est donc pas identiquement nul (mod. p).

Si nous convenons, comme il est naturel, de ne pas tenir compte, en évaluant le degré d'un polynome, des termes dont les coefficients sont nuls (mod. p), nous voyons que si l'on a

$$f(x)\,g(x) \equiv \varphi(x) \pmod{p},$$

le degré de $\varphi(x)$ est égal à la somme des degrés de f et de g. Nous dirons que $\varphi(x)$ est divisible par $f(x)$ (mod. p) : $g(x)$ est le quotient (mod. p) de $\varphi(x)$ par $f(x)$.

Comme dans la suite de ce chapitre il sera presque exclusivement

question de polynomes nuls (mod. p) ou divisibles l'un par l'autre (mod. p), etc., *nous sous-entendrons souvent l'indication* « (mod. p) ». Les détails dans lesquels nous sommes entrés jusqu'ici rendront sans doute toute confusion impossible. *Ainsi lorsque nous dirons simplement que $f(x)$ est divisible par $\varphi(x)$, il faudra sous-entendre :* (mod. p); lorsque nous voudrons dire que $f(x)$ est divisible par $\varphi(x)$, au sens ordinaire de l'algèbre, nous emploierons l'expression : « *algébriquement divisible* ».

Cela posé, nous allons montrer tout d'abord que, étant donnés deux polynomes $f(x)$ et $\varphi(x)$, et le degré de φ étant inférieur au degré de f, on peut toujours déterminer des polynomes $Q(x)$ et $R(x)$ tels que l'on ait

$$f(x) \equiv \varphi(x)\, Q(x) + R(x),$$

le degré de $R(x)$ *étant inférieur à celui de* $\varphi(x)$. On suppose, bien entendu, que $\varphi(x)$ n'est pas identiquement nul.

Il est clair que si le coefficient du terme de degré le plus élevé dans $\varphi(x)$ est égal à l'unité, il suffit d'effectuer la division *algébrique* de $f(x)$ par $\varphi(x)$ pour obtenir un résultat de cette forme. En effet, d'après la règle de la division, on n'aura jamais à écrire que des nombres entiers.

Il est facile de ramener à ce cas particulier celui où le premier coefficient de $\varphi(x)$ a une valeur quelconque a (*non nulle*). Soit a' l'associé de a; $a'\varphi(x)$ sera congru à un polynome $\varpi(x)$ dans lequel le premier coefficient sera égal à l'unité. Divisons $f(x)$ par $\varpi(x)$; nous aurons

$$f(x) \equiv \varpi(x)\, S(x) + T(x),$$

d'où

$$f(x) \equiv \varphi(x) . a'S(x) + T(x).$$

On peut d'ailleurs procéder différemment ; il suffit de multiplier $f(x)$ ou chaque dividende partiel par un nombre tel que la division soit possible sans introduire de fraction ; on obtient ainsi une égalité de la forme

$$A f(x) \equiv \varphi(x) . S(x) + T(x),$$

et si nous désignons par A' l'associé de A, nous aurons

$$f(x) \equiv \varphi(x) . A'S(x) + A'T(x).$$

Enfin, il est clair qu'on peut également effectuer la division algébriquement, sans s'inquiéter des nombres fractionnaires, et dans le résultat final, considérer ces nombres fractionnaires comme des

symboles et les remplacer par les nombres entiers équivalents. ainsi que nous l'avons expliqué dans la théorie des congruences du premier degré. Ce procédé serait surtout avantageux si l'on avait à effectuer une même division suivant plusieurs modules différents. Par exemple, on a *algébriquement*

$$4x^3 + 1 = (2x - 1)\left(2x^2 + x + \frac{1}{2}\right) + \frac{3}{2}.$$

Donc en remarquant que l'on a

$$\frac{3}{2} \equiv 0 \qquad (\text{mod. } 3),$$

$$\frac{1}{2} \equiv 2 \qquad (\text{mod. } 3),$$

on en conclut

$$4x^3 + 1 \equiv (2x - 1)(2x^2 + x + 2) \qquad (\text{mod. } 3).$$

De même, en tenant compte des congruences

$$\frac{3}{2} \equiv 5 \qquad (\text{mod. } 7),$$

$$\frac{1}{2} \equiv 4 \qquad (\text{mod. } 7),$$

on aurait

$$4x^3 + 1 \equiv (2x - 1)(2x^2 + x + 4) + 5 \qquad (\text{mod. } 7).$$

17. Le théorème fondamental sur lequel repose, comme en algèbre, toute la théorie du plus grand commun diviseur est le suivant :

Lorsqu'on a mis, comme il vient d'être expliqué, $f(x)$ sous la forme

$$f(x) = \varphi(x)\,Q(x) + R(x),$$

les diviseurs communs à f et à φ sont les mêmes que les diviseurs communs à φ et à R.

La démonstration s'appuie de même qu'en algèbre sur des théorèmes élémentaires qu'on peut résumer ainsi : *le polynome $\varphi(x)$ divisant $f(x)$* et *$g(x)$ divise aussi* $Af + Bg$, A *et* B *étant deux nombres ou polynomes quelconques.* Il semble inutile de s'attarder plus longuement sur ces éléments ; contentons-nous d'énoncer les propositions essentielles, en indiquant seulement les *différences* des démonstrations avec celles que l'on donne en algèbre.

Il résulte clairement du théorème fondamental que pour que $f(x)$ soit divisible par $\varphi(x)$, il faut et il suffit que $R(x)$ soit identique-

ment nul ; car $R(x)$ est de degré inférieur à celui de φ. (On aurait pu aussi déduire ce résultat de la théorie algébrique de la division).

On voit également qu'il existe ici un algorithme du plus grand commun diviseur, en tous points semblable à celui qui est connu en algèbre et en arithmétique élémentaire. Les diviseurs communs à deux polynomes sont aussi tous les diviseurs de leur plus grand commun diviseur.

Enfin il résulte également de la suite même des opérations qu'on exécute que si des polynomes f et g de degrés m et n ont un plus grand commun diviseur D de degré μ, il existe des polynomes f_1 et g_1, dont les degrés respectifs sont *inférieurs* à $m-\mu$ et $n-\mu$ et tels que l'on ait

$$fg_1 + gf_1 \equiv D.$$

En particulier si D est une constante, c'est-à-dire si les polynomes sont *premiers entre eux*, il existe des polynomes f_1 et g_1 de degrés *au plus égaux* à $m-1$ et $n-1$ et tels que l'on ait

$$fg_1 + gf_1 \equiv 1,$$

comme on le voit en multipliant les deux membres de la congruence précédente par l'associé de D.

Les propriétés du plus grand commun diviseur permettent de démontrer comme en arithmétique ou en algèbre toutes les propositions relatives à la divisibilité ; par exemple : *on ne change pas le plus grand commun diviseur de deux polynomes, en multipliant l'un d'eux par un polynome premier avec l'autre*, et en particulier : *si un polynome divise un produit de deux facteurs et est premier avec l'un d'eux, il divise l'autre*. Signalons encore ce théorème très important : *si un polynome est divisible par plusieurs autres premiers entre eux deux à deux, il est divisible par leur produit.*

Pour compléter l'analogie de cette théorie avec celle de la divisibilité des nombres entiers, il nous reste à introduire la notion qui correspond à celle de nombre premier, c'est-à-dire de nombre n'admettant pas d'autres diviseurs que lui-même et l'unité. Nous appellerons *polynome irréductible*(*) un polynome qui n'admet que des diviseurs d'un degré égal au sien ou de degré zéro, c'est-à-dire qui ne

(*) Il s'agit, bien entendu, de l'*irréductibilité* suivant le module p par rapport auquel on considère les congruences ; nous supprimons les mots (mod. p), comme on l'a expliqué au § 16.

peut pas être décomposé en un produit de deux facteurs polynomes. Il est sûr que les polynomes du premier degré satisfont à cette définition; mais il est facile de constater qu'ils ne sont pas les seuls. Considérons par exemple le polynome $x^3 - 2$ (mod. 7). Il est clair que, si ce polynome n'est pas irréductible, il admet au moins un diviseur du premier degré. Or, si l'on avait

$$x^3 - 2 \equiv (ax + b)(\alpha x^2 + \beta x + \gamma),$$

on pourrait poser, a n'étant certainement pas nul (mod. 7),

$$x_0 \equiv -\frac{b}{a} \qquad \text{(mod. 7)},$$

et il en résulterait

$$x_0^3 - 2 \equiv 0 \qquad \text{(mod. 7)}.$$

Or on voit aisément que $x_0^3 - 2$ ne peut pas être divisible par 7, quelque valeur entière que l'on donne à x_0. Il suffit pour s'en convaincre, de chercher, par la méthode de tâtonnements dont il a été déjà question, les racines de la congruence

$$x^3 - 2 \equiv 0 \qquad \text{(mod. 7)}.$$

On constate qu'*elle n'en a pas*. Le polynome donné est donc irréductible (mod. 7).

II. — Polynomes irréductibles.

18. La propriété caractéristique des polynomes irréductibles est la même que celle des nombres premiers : *Si f est un polynome irréductible et* F *un polynome quelconque, ou f divise* F, *ou f est premier avec* F. On en conclut qu'*un polynome irréductible ne peut diviser un produit de facteurs que s'il divise au moins l'un des facteurs*, ce qui permet d'énoncer la condition pour que deux produits de facteurs irréductibles soient divisibles l'un par l'autre et de montrer qu'*un polynome ne peut être décomposé que d'une seule manière en produit de facteurs irréductibles.* (Nous faisons, bien entendu, abstraction des facteurs numériques).

Il est facile de se rendre compte, au moins théoriquement, de quelle manière on peut effectuer cette décomposition. Il y a p polynomes irréductibles distincts du premier degré : x, $x+1$, $x+2$, ..., $x+p-1$; on cherchera d'abord si le polynome pro-

posé est divisible par l'un d'eux et on effectuera la division, si elle est possible ; on opérera de même sur le quotient et on continuera ainsi jusqu'à ce qu'on arrive à un quotient qui ne soit plus divisible par aucun des polynomes irréductibles du premier degré ; on aura mis ainsi le polynome donné $f(x)$ sous la forme

$$f(x) \equiv (x+\alpha_1)(x+\alpha_2) \ldots (x+\alpha_k) f_1(x),$$

$f_1(x)$ n'admettant plus que des facteurs irréductibles d'un degré supérieur au premier.

On pourrait diviser successivement $f_1(x)$ par tous les polynomes irréductibles du second degré, puis du troisième, etc., mais ce procédé exige que l'on connaisse ces polynomes. Si on ne les connait pas, on divisera $f_1(x)$ par les p^2 polynomes distincts du second degré, sans se préoccuper s'ils sont ou non irréductibles ; si $f_1(x)$ est divisible par l'un d'eux, celui-là est certainement irréductible, car sinon il admettrait un diviseur du premier degré, lequel diviserait $f_1(x)$, ce qui est contraire à l'hypothèse. (Ces p^2 polynomes distincts du second degré s'obtiennent en donnant séparément à α et β, dans l'expression $x^2+\alpha x+\beta$, p valeurs formant un système complet de nombres incongrus). On passera de même aux diviseurs du troisième degré après avoir épuisé ceux du second, et ainsi de suite jusqu'à ce que l'on arrive à un polynome $g(x)$, de degré h, qui ne soit divisible par aucun polynome de degré inférieur ou égal à $\frac{h}{2}$; ce polynome $g(x)$ sera nécessairement irréductible.

On peut d'ailleurs montrer que le nombre des polynomes irréductibles est illimité par un raisonnement tout à fait pareil à celui par lequel on démontre que la suite des nombres premiers est illimitée. Comme le nombre des polynomes *distincts* de chaque degré est limité, on en conclut qu'il existe des polynomes irréductibles dont le degré dépasse tout nombre donné à l'avance. Nous démontrerons plus loin qu'il existe des polynomes irréductibles de *tous* les degrés.

19. Ces résultats étant acquis, nous pouvons aborder l'étude des congruences en général. Si nous cherchons à continuer l'analogie de cette théorie avec l'algèbre, la proposition suivante s'offre d'abord à nous : *Pour qu'une congruence*

$$f(x) \equiv 0 \qquad (\text{mod. } p)$$

admette la racine $x \equiv a$, *il faut et il suffit que son premier membre soit divisible par* $x - a$.

En effet, on a, *algébriquement*,

$$f(x) = (x - a)Q(x) + f(a).$$

Donc on a

$$f(x) \equiv (x - a)Q(x) + f(a) \qquad (\text{mod. } p),$$

formule qui pouvait d'ailleurs être établie directement et d'où l'on déduit le théorème énoncé. Il résulte de là qu'*une congruence irréductible* (c'est-à-dire dont le premier membre est un polynome irréductible dont le degré dépasse l'unité) *n'a pas de racines* (*).

En général on peut dire que : *le nombre des racines d'une congruence est égal au nombre des facteurs irréductibles du premier degré de son premier membre* (on tient compte, bien entendu, des *facteurs multiples* en attribuant aux racines correspondantes un *degré de multiplicité*).

Une congruence ne peut donc avoir plus de racines qu'il n'y a d'unités dans son degré. Par exemple, la congruence

$$x^3 + 2x^2 - 3 \equiv 0 \qquad (\text{mod. } 7)$$

a trois racines ; car on a

$$x^3 + 2x^2 - 3 \equiv (x - 1)^2(x - 3) \qquad (\text{mod. } 7) ;$$

au contraire la congruence

$$x^3 + 5x^2 + x - 2 \equiv 0 \qquad (\text{mod. } 7)$$

a une seule racine, car on a

$$x^3 + 5x^2 + x - 2 \equiv (x^2 + 1)(x - 2) \qquad (\text{mod. } 7)$$

et le binome $x^2 + 1$ est irréductible (mod. 7).

On voit l'importance qu'il y aurait à connaitre une méthode directe permettant de trouver sans tâtonnements les facteurs irréductibles du premier degré d'un polynome donné. Nous supposerons que tous ces facteurs du premier degré sont simples ; on verrait en effet facilement qu'on peut transporter ici sans modification la méthode dite « des racines égales ». On voit immédiatement, en effet que lorsque deux polynomes sont congrus, il en est de même de leurs dérivées d'ordre quelconque, et l'on peut de plus ajouter que cette proposition sub-

---

(*) Il semble, au premier abord, qu'il y ait là une différence très profonde avec l'algèbre ; il ne faut pas trop s'en étonner ; nous n'avons en effet encore rien introduit qui corresponde à la notion des nombres algébriques; nous verrons plus loin qu'en réalité, il y a ici avec l'algèbre une différence moins grande qu'il ne parait tout d'abord.

siste, si on remplace les dérivées d'ordre k par leur quotient par $k!$ Il suffit, en effet, de remarquer que $\frac{f^k(x)}{k!}$ est *par définition* le coefficient de h^k dans le développement de $f(x+h)$ suivant les puissances croissantes de h (*).

Considérons donc un polynome $f(x)$ n'ayant que des facteurs simples du premier degré ; il est clair que le produit de ces facteurs est le plus grand commun diviseur du polynome proposé et du polynome

$$\varphi(x) = x(x+1)(x+2)\ldots(x+p-1).$$

Si nous posons

$$\varphi(x) = x^p + A_1 x^{p-1} + A_2 x^{p-2} + \ldots + A_{p-1}x,$$

et par suite,

$$\begin{aligned}\varphi(x+1) = {} & x^p + \frac{p}{1}x^{p-1} + \ldots + \frac{p(p-1)\ldots(p-k+1)}{k!}x^{p-k} + \ldots\ldots + \frac{p}{1}x + 1\\ & + A_1 x^{p-1} + \ldots + A_1\frac{(p-1)\ldots(p-k+1)}{(k-1)!}x^{p-k} + \ldots\ldots + A_1\frac{p-1}{1}x + A_1\\ & + \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ & + A_{p-2}x^2 + A_{p-2}\,2x + A_{p-2}\\ & + A_{p-1}\,x + A_{p-1},\end{aligned}$$

nous aurons, en écrivant l'identité

$$x\varphi(x+1) = (x+p)\varphi(x),$$

les relations

$$A_2 + pA_1 = A_2 + \frac{p-1}{1}A_1 + \frac{p(p-1)}{2},$$

$$A_3 + pA_2 = A_3 + \frac{p-2}{1}A_2 + \frac{(p-1)(p-2)}{1.2}A_1 + \frac{p(p-1)(p-2)}{1.2.3},$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$pA_{p-1} = A_{p-1} + A_{p-2} + \ldots + A_2 + A_1 + 1,$$

(*) Une petite difficulté se présente dans la méthode des racines égales lorsque, les exposants de tous les termes d'un polynome $f(x)$ étant des multiples de p, $f'(x)$ est identiquement nul (mod. p). On voit facilement que dans ce cas, on doit supprimer les facteurs p introduits par la dérivation ; si tous les exposants dans $f(x)$ sont divisibles par p^2, on considérera $\frac{1}{p^2}f''(x)$ au lieu de $f''(x)$.

qui permettraient de calculer de proche en proche les coefficients A. Au lieu de faire ce calcul, nous remarquerons que l'expression

$$\frac{p(p-1)(p-2)\ldots(p-k+1)}{k!},$$

qui, comme on le sait, est un nombre entier, est divisible par p lorsque p est un nombre premier; en effet, k étant inférieur à p, le facteur premier p entre une fois en facteur au numérateur et n'entre pas au dénominateur. Il résulte alors de nos équations

$$\left\{\begin{array}{l} A_1 \equiv 0, \\ A_2 \equiv 0, \\ \ldots\ldots\ldots \\ \ldots\ldots\ldots \\ A_{p-2} \equiv 0, \\ A_{p-1} \equiv -1, \end{array}\right. \qquad (\text{mod. } p),$$

et par suite

$$\varphi(x) \equiv x^p - x \qquad (\text{mod. } p).$$

Nous aurions pu facilement prévoir ce résultat; en effet, d'après le théorème de Fermat, la congruence

$$x^p - x \equiv 0$$

admet les p racines distinctes $0, 1, 2, \ldots, p-1$, ou $0, -1, -2, \ldots, -p+1$; on a donc

$$x^p - x \equiv (x+p-1)(x+p-2)\ldots(x+2)(x+1)x.$$

Ce calcul constitue d'ailleurs une nouvelle démonstration du théorème de Fermat, ayant pour base la formule du binome et la remarque faite sur ses coefficients. Il existe une démonstration plus simple fondée sur le même principe: on a

$$(a+b)^p \equiv a^p + b^p \qquad (\text{mod. } p),$$

d'où

$$(a+b)^p - (a+b) \equiv a^p - a + b^p - b \qquad (\text{mod. } p).$$

Le théorème de Fermat est donc vrai pour la somme de deux nombres, lorsqu'il est vrai pour ces deux nombres; comme il est vrai pour *l'unité*, il est toujours vrai.

La formule identique

$$(x+1)\ldots(x+p-1) \equiv x^{p-1} - 1 \qquad (\text{mod. } p)$$

conduit également à plusieurs autres conséquences intéressantes; en

égalant les termes constants dans les deux membres on obtient

$$1.2\ldots(p-1) \equiv -1 \qquad (\text{mod. } p),$$

c'est-à-dire le théorème de Wilson. En égalant les coefficients des diverses puissances de x on voit que les autres fonctions symétriques élémentaires (sommes des produits h à h ; $h < p-1$) des $p-1$ premiers nombres entiers sont divisibles par p. En se servant des formules de Newton, qui donnent les sommes des puissances semblables de plusieurs quantités en fonction de leurs fonctions symétriques élémentaires, on reconnait que la somme des $m^{\text{ièmes}}$ puissances des $p-1$ premiers nombres entiers est divisible par p, à moins que m ne soit un multiple de $p-1$.

Ainsi pour trouver le produit de tous les facteurs du premier degré d'un polynome, pris chacun une seule fois, il suffit de chercher le plus grand commun diviseur de ce polynome et de $x^p - x$ (ou, si l'on veut, de $x^{p-1}-1$, en supprimant la racine nulle, ce qu'on peut toujours faire). Le degré de ce plus grand commun diviseur est égal au nombre des racines inégales de la congruence obtenue en égalant ce polynome à zéro.

Comme application, cherchons le nombre des racines de la congruence

$$x^n - D \equiv 0 \qquad (\text{mod. } p),$$

en supposant que n soit un diviseur de $p-1$.

Posons $p-1 = n\delta$; nous avons

$$x^{p-1}-1 = x^{n\delta}-1 \equiv (x^n - D)(x^{n(\delta-1)} + Dx^{n(\delta-2)} + \ldots + D^{\delta-2}x^n + D^{\delta-1}) + D^{\delta} - 1.$$

Donc si l'on a

$$D^{\delta} \equiv 1 \qquad (\text{mod. } p),$$

le plus grand commun diviseur est $x^n - D$ et la congruence proposée a n racines. Au contraire, *si l'on n'a pas*

$$D^{\delta} \equiv 1 \qquad (\text{mod. } p),$$

la congruence proposée n'a aucune racine.

Il convient d'énoncer, à cause de sa grande importance, cette conséquence évidente des propositions déjà démontrées : *si une congruence a autant de racines qu'il y a d'unités dans son degré, il en est de même de toute congruence dont le premier membre est un diviseur du premier membre de la congruence proposée.*

Il est aisé de voir que l'analogie de la théorie précédente avec la

théorie des équations serait complète si l'on excluait de cette dernière le concept de nombre algébrique. Si l'on ne considère, en effet, que les racines entières ou fractionnaires des équations, chaque équation algébrique entière à coefficients entiers a tout juste autant de racines que son premier membre admet de diviseurs rationnels du premier degré.

Ce point de vue un peu étroit a été depuis longtemps abandonné en algèbre ; les recherches de Galois (1831) permettent aussi, dans la théorie des congruences, de se placer à un point de vue plus élevé.

III. — Théorie des congruences au point de vue de Galois.

20. Soit d'une manière générale $f(x) \equiv 0 \pmod{p}$ une congruence dont nous supposons le premier membre irréductible (mod. p). Nous supposons donc qu'il n'existe aucune identité de la forme

$$f(x) = \mathrm{P}(x)\,\mathrm{Q}(x) + p\mathrm{R}(x)$$

où les polynomes P, Q, R sont à coefficients entiers.

Il n'existe aucun entier qui, mis à la place de x, vérifie la congruence. Galois a été conduit par là à introduire dans le calcul de nouveaux symboles, suivant les mêmes règles de calcul que les entiers ordinaires, et vérifiant chacun une congruence de cette nature. Nous développerons dans une Note la conception de Galois d'une manière précise et systématique ; pour le moment, nous observons que le calcul d'un symbole i pour lequel on a, *par définition*,

$$f(i) \equiv 0 \pmod{p}$$

est au fond identique avec celui d'un entier *indéterminé* i, si l'on convient de négliger les multiples de $f(i)$: en d'autres termes, c'est l'étude des polynomes entiers en x et i à coefficients entiers, en négligeant à la fois les multiples de p et de $f(i)$.

On est amené ainsi à un point de vue auquel Kronecker s'est constamment placé, en lui donnant d'ailleurs une grande extension; voici comment, de ce point de vue, se présente la théorie des *imaginaires de Galois*. Étant donnés un nombre entier p et un polynome $f(z)$, on dira que deux polynomes $\varphi(z)$, $\psi(z)$ sont congrus *suivant le système de modules* p, $f(z)$, et l'on écrira

$$\varphi(z) \equiv \psi(z) \quad (\text{modd. } p, f(z)),$$

lorsque la différence $\varphi(z) - \psi(z)$ pourra se mettre sous la forme $Ap + Bf(z)$, A et B étant des polynomes entiers en z. Il est à peine utile de rappeler que tous les polynomes que nous considérons doivent avoir leurs coefficients entiers.) Cette définition revient à dire que la différence $\varphi(z) - \psi(z)$ est divisible par $f(z)$ suivant le module p. On voit de suite que, relativement à l'addition et la multiplication, les congruences suivant un système de modules suivent les mêmes lois que les égalités ordinaires, ou que les congruences ordinaires relatives à des nombres et à un seul module.

Les congruences qu'on vient de définir sont l'analogue des congruences entre des *nombres* ; on peut de même considérer des congruences [suivant le système de modules $p, f(z)$] qui contiennent des inconnues. Soit $F(x, z)$ un polynome entier en x et z ; on appellera solution de la congruence

$$F(x, z) \equiv 0 \qquad [\text{modd. } p, f(z)],$$

tout polynome $\varphi(z)$ tel que le polynome obtenu en mettant $\varphi(z)$ à la place de x dans $F(x, z)$ soit congru à 0 suivant le système de modules $p, f(z)$, c'est-à-dire divisible par $f(z)$ (mod. p).

Ces définitions admises, et regardant maintenant la lettre i comme une indéterminée que nous écrirons à la place de z, p étant un nombre premier, et le polynome $f(x)$ étant supposé irréductible (mod. p), nous appellerons imaginaire de Galois tout polynome en i ; deux imaginaires de Galois $\varphi(i)$, $\psi(i)$ seront dites égales quand on aura, au sens précédemment défini,

$$\varphi(i) \equiv \psi(i) \qquad [\text{modd. } p, f(i)].$$

Soit $F(x)$ un polynome en x dont les coefficients peuvent être des imaginaires de Galois ; la congruence

$$F(x) \equiv 0 \qquad [\text{modd. } p, f(i)]$$

admettra la solution $\varphi(i)$ si le polynome $F[\varphi(i)]$ est *nul* [modd. p, $f(i)$] ; dans ce sens il est clair que la congruence

$$f(x) \equiv 0 \qquad [\text{modd. } p, f(i)]$$

admet la solution $x = i$. La congruence $f(x) \equiv 0$ est dite fondamentale.

D'après les hypothèses faites sur le symbole i, nous pourrons à l'aide de l'équation

$$f(i) \equiv 0 \qquad (\text{mod. } p)$$

ramener toute *imaginaire de Galois* à la forme

$$g \equiv a_0 + a_1 i + a_2 i^2 + \ldots + a_{n-1} i^{n-1} \qquad (\text{mod. } p).$$

en désignant par n le degré de $f(i)$ et par $a_0, a_1, \ldots, a_{n-1}$ des nombres entiers que nous pouvons supposer compris entre 0 et $p - 1$.

Il n'y a donc qu'un nombre limité d'imaginaires distinctes, à savoir, par exemple, les imaginaires qui se déduisent de l'expression

$$a_0 + a_1 i + \ldots + a_{n-1} i^{n-1}$$

en donnant à $a_0, a_1, \ldots, a_{n-1}$ les valeurs $0, 1, 2, \ldots, p - 1$, ce qui fournit p^n imaginaires distinctes [modd. p, $f(i)$], dont une seule est nulle [modd. p, $f(i)$].

La propriété que possède un polynome irréductible, de ne pouvoir diviser un produit de facteurs sans diviser au moins l'un des facteurs devient, avec les conventions de langage que nous avons faites : *un produit de facteurs réels ou imaginaires ne peut être nul que si l'un des facteurs est nul.* [*Nul* signifiant *congru à zéro suivant le double module* p, $f(i)$].

Il en résulte que si A et B sont deux imaginaires distinctes, dont la première n'est pas nulle [modd. p, $f(i)$], et si dans $Ax + B$, on substitue, à la place de x, p^n imaginaires distinctes, on aura p^n imaginaires distinctes ; il y a donc une imaginaire et une seule qui satisfait à la congruence

$$Ax + B \equiv 0 \qquad [\text{modd. } p, f(i)],$$

c'est-à-dire que, suivant le système de modules p, $f(i)$, une imaginaire quelconque est divisible par une imaginaire quelconque non nulle.

L'ensemble des imaginaires distinctes et non nulles constitue un *groupe limité*, en ce sens que le produit de deux éléments du groupe est un élément du groupe. En particulier si dans l'expression Ax, où A n'est pas nul, on met à la place de x tous les éléments de ce groupe, on retrouve tous les éléments du groupe ; et on obtient, comme dans la théorie des nombres entiers, le théorème qu'exprime la congruence

$$A^{p^n-1} - 1 \equiv 0 \qquad [\text{modd. } p, f(i)];$$

il en résulte que l'on a, quelle que soit l'imaginaire de Galois A,

$$A^{p^n} - A \equiv 0 \qquad [\text{modd. } p, f(x)],$$

ce qui revient à dire que, quel que soit le polynome $\theta(x)$, le polynome

$$\theta^{p^n}(x) - \theta(x)$$

est divisible (mod. p) par $f(x)$ pourvu que le polynome de degré n $f(x)$ soit irréductible (mod. p).

A chaque imaginaire A correspond aussi une imaginaire *associée* A' telle que l'on ait

$$AA' \equiv 1 \qquad [\text{modd. } p, f(i)],$$

et cette remarque conduit aisément à une généralisation du théorème de Wilson.

21. Ceci posé, conservons toujours le même sens à p et à $f(i)$. Si $\varphi(x)$ est un polynome entier en x et i, on dira que l'imaginaire $\theta(i)$ est une racine de la congruence

$$\varphi(x) \equiv 0 \qquad [\text{modd. } p, f(i)],$$

si en remplaçant dans $\varphi(x)$, x par $\theta(i)$, la congruence est vérifiée. Un polynome $\varphi(x)$ est identiquement nul [modd. p, $f(i)$] si tous ses coefficients sont nuls [modd. p, $f(i)$]; deux polynomes entiers en x et i sont congrus [modd. p, $f(i)$] si leur différence est identiquement nulle [modd. p, $f(i)$].

Le produit de deux polynomes, $\varphi(x)$ et $\psi(x)$, entiers en x et i ne peut être identiquement nul [modd. p, $f(i)$], que si l'un des polynomes est identiquement nul par rapport au même système de modules. Il suffit, comme on l'a fait plus haut, dans un théorème analogue, de considérer le produit des termes de plus haut degré en x dans les deux polynomes, en négligeant bien entendu les coefficients qui seraient nuls [modd. p, $f(i)$]. Et l'on voit que, dans ces conditions, le degré du polynome produit est la somme des degrés des deux facteurs : le degré est l'exposant de x dans le terme du plus haut exposant dont le coefficient n'est pas nul [modd. p, $f(i)$].

Un polynome $\varphi(x)$ entier en x et i est divisible [modd. p, $f(i)$] par un polynome $\psi(x)$, entier en x et i, s'il existe un polynome $\chi(x)$ entier en x et i tel que l'on ait

$$\varphi(x) \equiv \psi(x)\chi(x) \qquad [\text{modd. } p, f(i)].$$

Cela est impossible quand $\varphi(x)$ est de degré inférieur à $\psi(x)$, à moins que $\varphi(x)$ ne soit identiquement nul [modd. p, $f(i)$]. Si $\varphi(x)$ est de degré supérieur à $\psi(x)$, on peut mettre $\varphi(x)$ sous la forme

$$\varphi(x) \equiv \psi(x)\,Q(x) + R(x) \qquad [\text{modd.}\, p,\ f(i)],$$

$Q(x)$ et $R(x)$ étant, comme $\varphi(x)$ et $\psi(x)$, des polynomes entiers en x et i et $R(x)$ étant de degré inférieur à $\psi(x)$.

On a maintenant tous les éléments pour faire une théorie de la divisibilité des polynomes entiers en x et i, suivant le système de modules p, $f(i)$, toute pareille à celle que l'on a indiquée, pour les polynomes entiers en x, par rapport au module p. On aura le même algorithme pour le plus grand commun diviseur [modd. p, $f(i)$], les mêmes conséquences, la notion de polynome en x, i irréductible [modd. p, $f(i)$], la décomposition unique en facteurs irréductibles [modd. p, $f(i)$] et les mêmes conséquences relatives à la divisibilité. Mais outre qu'une confusion serait à craindre, par une attribution de deux sens au mot *irréductible*, l'étude complète et approfondie de la divisibilité des polynomes à coefficients imaginaires nous entraînerait trop loin. Aussi allons-nous considérer seulement *les facteurs imaginaires du premier degré, de la forme* $x - g$ *et conserver au mot irréductible son sens primitif.*

On démontre aisément, comme lorsqu'il s'agit des facteurs réels, que si une congruence admet les racines distinctes $g_1, g_2, \ldots, g_q$, son premier membre est divisible par le produit $(x-g_1)(x-g_2)\ldots(x-g_q)$ et on en conclut qu'une congruence ne peut pas avoir plus de racines qu'il n'y a d'unités dans son degré. Le nombre des racines ainsi définies est égal au nombre des facteurs du premier degré. Tout cela se conclut très facilement du fait que le produit de deux imaginaires ne peut être nul que si un des facteurs est nul.

Il convient de faire ici une remarque importante : les racines communes à deux polynomes (à coefficients réels) appartiennent à leur plus grand commun diviseur (mod. p) ; en effet, si D désigne le plus grand commun diviseur de F et G, on peut trouver des polynomes f_1 et g_1 tels que

$$Fg_1 + Gf_1 \equiv D \qquad (\text{modd.}\, p) ;$$

on a donc *a fortiori*

$$Fg_1 + Gf_1 \equiv D \qquad [\text{modd.}\, p,\ f(i)],$$

ce qui démontre la proposition énoncée. En particulier, si $F(x)$ désigne un polynome irréductible et si la congruence

$$\Phi(x) \equiv 0 \qquad [\text{modd.}\, p,\ f(i)]$$

admet une racine (imaginaire) de la congruence

$$F(x) \equiv 0 \qquad [\text{modd. } p, f(i)],$$

$\Phi(x)$ est divisible par $F(x)$ suivant le module p.

En particulier deux polynomes irréductibles ne peuvent pas avoir de racine commune et un polynome irréductible ne peut pas avoir de racine multiple, puisqu'il est premier avec sa dérivée.

22. Pour obtenir sans tâtonnements les facteurs du premier degré d'une congruence donnée, ou du moins leur produit, il suffira de chercher le plus grand commun diviseur du premier membre de la congruence proposée avec le produit *de tous les facteurs distincts du premier degré*. Ce produit nous est fourni par la généralisation du théorème de Fermat ; nous avons vu, en effet, que la congruence

$$x^{p^n} - x \equiv 0 \qquad [\text{modd. } p, f(i)]$$

avait pour racines les p^n valeurs distinctes de l'imaginaire γ ; le produit des p^n facteurs tels que $x - \gamma$ est donc congru à $x^{p^n} - x$.

En particulier si la congruence proposée est irréductible, pour qu'elle admette une racine, il faut qu'elle ait une racine commune avec $x^{p^n} - x$, il faut donc que son premier membre divise $x^{p^n} - x$. D'ailleurs il est clair que tout diviseur de $x^{p^n} - x$ a autant de racines qu'il y a d'unités dans son degré. Donc, au point de vue où nous nous plaçons, une congruence irréductible *ou n'a pas de racines, ou a autant de racines qu'il y a d'unités dans son degré* ; ce dernier cas se présente lorsque le premier membre de la congruence proposée est un diviseur de $x^{p^n} - x$.

En particulier, la congruence

$$f(x) \equiv 0 \qquad [\text{modd. } p, f(i)]$$

admet la racine

$$x \equiv i ;$$

donc elle admet n racines et $f(x)$ divise $x^{p^n} - x$. Or $f(x)$ est un polynome quelconque irréductible de degré n. Donc tout polynome irréductible de degré n divise $x^{p^n} - x$ et par suite admet n racines imaginaires. Il est clair que si r est un diviseur de n, tout polynome irréductible de degré r divise $x^{p^r} - x$ et par suite $x^{p^n} - x$ (car $x^{p^n - 1} - 1$ est alors divisible *algébriquement* par $x^{p^r - 1} - 1$, puisque $p^n - 1$ est divisible par $p^r - 1$). Donc *toute congruence irréductible dont le degré est égal à n ou à un diviseur de n a autant de racines qu'il y a d'unités dans son degré.*

Nous allons montrer maintenant qu'une congruence de degré m n'a pas de racines, lorsque m n'est pas un diviseur de n. Il suffit de montrer que $x^{p^n} - x$ ne peut pas être divisible par un polynome irréductible dont le degré n'est pas un diviseur de n.

Pour cela une remarque préliminaire est nécessaire. Nous avons vu que l'on a identiquement

$$(a + b)^p \equiv a^p + b^p \pmod{p}.$$

Il en résulte l'identité

$$(a + bx + cx^2 + \dots + hx^n)^p \equiv a^p + b^p x^p + c^p x^{2p} + \dots + h^p x^{np} \pmod{p};$$

or on a

$$a^p \equiv a \pmod{p},$$
$$b^p \equiv b \pmod{p},$$
$$\dots\dots$$
$$\dots\dots$$
$$h^p \equiv h \pmod{p},$$

d'après le théorème de Fermat. Donc on a

$$(a + bx + cx^2 + \dots + hx^n)^p \equiv a + bx^p + cx^{2p} + \dots + hx^{np} \pmod{p},$$

c'est-à-dire que, $\varphi(x)$ désignant un polynome quelconque, on a

$$[\varphi(x)]^p \equiv \varphi(x^p) \pmod{p}.$$

En remplaçant x par x^p, on a

$$\varphi(x^{p^2}) \equiv [\varphi(x^p)]^p \equiv [\varphi(x)]^p]^p \equiv [\varphi(x)]^{p^2} \pmod{p},$$

et généralement

$$[\varphi(x)]^{p^r} \equiv \varphi(x^{p^r}) \pmod{p}.$$

Nous pouvons maintenant démontrer qu'un polynome irréductible $f(x)$ de degré m ne peut pas diviser $x^{p^r} - x$ si r est inférieur à m.

Il s'agit en effet de prouver qu'on ne peut pas avoir

$$i^{p^r} \equiv i \quad [\text{modd. } p, f(i)].$$

Or si cette égalité avait lieu, en désignant *par* $\varphi(i)$ *une imaginaire quelconque* on aurait

$$\varphi(i^{p^r}) \equiv \varphi(i) \quad [\text{modd. } p, f(i)].$$

Or nous venons de voir que

$$\varphi(i^{p^r}) \equiv [\varphi(i)]^{p^r} \pmod{p};$$

on aurait donc

$$[\varphi(i)]^{p^r} \equiv \varphi(i) \quad [\text{modd. } p, f(i)],$$

c'est-à-dire que la congruence

$$x^{p^r} \equiv x \quad [\text{modd. } p, f(i)]$$

aurait pour racines *toutes les imaginaires* c'est-à-dire p^m racines, ce qui est impossible puisqu'elle est de degré p^r.

Il est facile de voir que, plus généralement, $f(x)$ ne peut diviser $x^{p^n} - x$ que si n est un multiple de m; sinon posons $n = mq + r$, r étant inférieur à m; l'expression

$$x^{p^{mq}} - x$$

est divisible par $f(x)$, suivant une remarque déjà faite; si $x^{p^{mq+r}} - x$ l'était aussi, il en serait de même de leur différence

$$x^{p^{mq+r}} - x^{p^{mq}}.$$

Or on a

$$x^{p^{mq+r}} - x^{p^{mq}} \equiv (x^{p^r} - x)^{p^{mq}} \qquad (\text{mod. } p).$$

L'hypothèse faite est donc inadmissible.

23. Considérons un nombre quelconque de congruences irréductibles (mod. p), de degrés a, b, c, .., l. Soit N le plus petit multiple commun de ces degrés; $F(x)$ une congruence irréductible (mod. p) de degré N; si nous introduisons l'imaginaire de Galois i définie par la relation

$$F(i) \equiv 0 \qquad (\text{mod. } p),$$

chacune des congruences proposées aura autant de racines qu'il y a d'unités dans son degré.

Comme un polynome quelconque peut toujours être décomposé en facteurs irréductibles, il en résulte qu'étant donné un nombre quelconque de congruences, on peut toujours définir une imaginaire de Galois de manière que chacune d'elles ait autant de racines qu'il y a d'unités dans son degré.

Nous avons fait implicitement une hypothèse, en admettant l'existence d'un polynome irréductible (mod. p) d'un degré quelconque N. Pour justifier cette hypothèse, nous allons calculer le nombre des polynomes irréductibles de degré n.

Nous savons que $x^{p^n} - x$ n'admet que des facteurs irréductibles dont le degré est n ou un diviseur de n et est divisible d'ailleurs par tous les polynomes irréductibles dont le degré est n ou un diviseur de n; d'ailleurs $x^{p^n-1} - 1$ est premier avec sa dérivée et par suite n'admet pas de facteurs multiples; il en est donc de même de $x^{p^n} - x$. *Donc* $x^{p^n} - x$ *est égal au produit de tous les polynomes irréductibles dont le degré est égal à* n *ou à un diviseur de* n. *Si nous désignons par* $\theta(n)$ *le degré du produit de tous les poly-*

nomes irréductibles de degré n, on a par suite

$$p^n = \Sigma\theta(d),$$

le signe Σ se rapportant à tous les diviseurs de n, y compris l'unité et n lui-même. Nous savons qu'en désignant par q, q', q'',... les facteurs premiers *distincts* de n, on déduit de cette formule :

$$\theta(n) = p^n - \Sigma p^{\frac{n}{q}} + \Sigma p^{\frac{n}{qq'}} - \Sigma p^{\frac{n}{qq'q''}} + \cdots$$

Le nombre des polynomes irréductibles de degré n est évidemment égal à $\frac{1}{n}\theta(n)$, c'est-à-dire à

$$\frac{1}{n}\left[p^n - \Sigma p^{\frac{n}{q}} + \Sigma p^{\frac{n}{qq'}} - \Sigma p^{\frac{n}{qq'q''}} + \cdots\right].$$

On vérifie assez facilement que cette expression est positive (*), ce qui démontre l'existence de polynomes irréductibles d'un degré quelconque n.

Il est évident que, de plus, elle doit être un nombre entier ; on a donc

$$p^n - \Sigma p^{\frac{n}{q}} + \Sigma p^{\frac{n}{qq'}} \cdots \equiv 0 \qquad (\text{mod. } n),$$

n étant un nombre quelconque et p un nombre premier. *Lejeune Dirichlet* a démontré que a et n étant premiers entre eux, il y a une infinité de nombres *premiers* p vérifiant la congruence

$$a \equiv p \qquad (\text{mod. } n).$$

Si on admet cette proposition de Lejeune Dirichlet, il en résulte que, a étant un nombre *quelconque premier avec* n, on a

$$a^n - \Sigma a^{\frac{n}{q}} + \Sigma a^{\frac{n}{qq'}} - \Sigma a^{\frac{n}{qq'q''}} + \cdots \equiv 0 \qquad (\text{mod. } n).$$

Si on suppose que n est un nombre premier, cette congruence exprime le théorème de *Fermat* ; on peut donc la regarder, dans le cas d'un module quelconque, comme une généralisation de ce théorème. Cette généralisation coïncide avec la proposition connue sous le nom de *théorème de Fermat généralisé*, dans le cas seulement où n est une puissance d'un nombre premier.

(*) En se servant de la formule $p^x = e^{x\log p} = 1 + \frac{x\log p}{1} + \frac{x^2\log^2 p}{1.2} + \ldots$ on trouve qu'elle est égale à

$$\frac{1}{n}\left[\frac{\log p}{1}\left(1-\frac{1}{q}\right)\left(1-\frac{1}{q'}\right)\ldots + \frac{\log^2 p}{1.2}\left(1-\frac{1}{q^2}\right)\left(1-\frac{1}{q'^2}\right)\ldots + \ldots\right].$$

CHAPITRE III

DES CONGRUENCES BINOMES

I. — Racines primitives et indices.

24. Revenant maintenant à un sujet beaucoup plus élémentaire, nous allons étudier une classe intéressante de congruences : les congruences binomes. Nous pourrions, comme nous l'avons déjà montré sur un exemple dans le chapitre précédent (§ 19) appliquer, sans les modifier, les méthodes générales à ces congruences particulières; mais il est préférable d'étudier la question directement.

Soit a un nombre entier non divisible par le nombre premier p; considérons la série des puissances de a :

$$(A) \qquad a^0 = 1, a, a^2, a^3, \ldots$$

et prenons leurs résidus minima par rapport à p. Le nombre des résidus minima étant limité et la suite (A) indéfinie, il y a nécessairement dans cette suite des termes ayant même résidu minimum, c'est-à-dire congrus entre eux. Soit a^r *le premier* des termes de la suite qui soit congru à l'un des précédents a^α. Je dis que l'on a nécessairement $\alpha = 0$; sinon de la congruence

$$a^r \equiv a^\alpha \pmod{p},$$

on déduirait, en divisant par a, qui n'est pas nul (mod. p),

$$a^{r-1} \equiv a^{\alpha-1},$$

c'est-à-dire que a^r ne serait pas le premier des termes congrus à l'un des précédents. On a donc

$$a^r \equiv a^0 \equiv 1 \pmod{p}$$

et *r est le plus petit nombre pour lequel cette congruence ait lieu.* On exprime ce fait en disant que le nombre *a appartient à l'exposant r* (relativement au nombre premier p). Il est clair que l'on a géné-

ralement

$$a^{nr} \equiv 1 \qquad (\text{mod. } p).$$

Réciproquement, pour que l'on ait

$$a^m \equiv 1 \qquad (\text{mod. } p),$$

il faut que m soit un multiple de r; en effet, si l'on avait $m = nr + q$, q étant inférieur à r, on en conclurait

$$a^q \equiv 1 \qquad (\text{mod. } p),$$

ce qui est impossible.

Il en résulte que la suite des résidus minima des puissances successives de a est *périodique*; les restes se reproduisent de r en r.

Dans ce qui précède, nous n'avons pas admis le théorème de Fermat; cela n'aurait guère simplifié d'ailleurs. Mais ce théorème nous montrerait immédiatement, d'après une remarque qui vient d'être faite, que $p-1$ est un multiple de r, ou mieux que : *l'exposant* r *auquel appartient un nombre quelconque* a *est un diviseur de* $p-1$. Mais nous préférons démontrer directement cette proposition importante parce que le mode de raisonnement que nous allons employer est d'un usage assez fréquent et qu'il est intéressant de le connaître. Nous pourrons ensuite en déduire comme corollaire le théorème de Fermat.

Nous avons dit que les r nombres

$$\text{(I)} \qquad 1,\ a,\ a^2,\ \ldots,\ a^{r-1}$$

sont incongrus (mod. p); comme aucun d'eux n'est congru à zéro, leur nombre est au plus égal à $p-1$. Il peut donc se faire que l'on ait

$$p - 1 = r.$$

Supposons, au contraire,

$$p - 1 > r,$$

et désignons par a' un nombre quelconque incongru à zéro et à tous les nombres de la suite (I). Considérons les r nombres

$$\text{(II)} \qquad a',\ a'a,\ a'a^2,\ \ldots,\ a'a^{r-1}.$$

Ils sont incongrus entre eux ; car si on avait

$$a'a^2 \equiv a'a^3 \qquad (\text{mod. } p),$$

on en conclurait

$$a^2 \equiv a^3 \qquad (\text{mod. } p),$$

ce qui est contraire à l'hypothèse. De plus un nombre quelconque de la suite (II) est incongru à un nombre quelconque de la suite (I),

car si on avait

$$a'a^{\alpha} \equiv a^{\beta} \qquad (\text{mod. } p),$$

on en déduirait

$$a' \equiv a^{\beta+r-\alpha},$$

ce qui est également contraire à l'hypothèse.

Les $2r$ nombres formant les suites (I) et (II) étant incongrus, $2r$ ne peut surpasser $p-1$; il peut se faire que l'on ait

$$p-1 = 2r;$$

si nous supposons

$$p-1 > 2r,$$

nous pourrons choisir un nombre a'' différent (mod. p) de zéro et des $2r$ nombres des suites (I) et (II) et nous formerons la suite

(III) $$a'', \; a''a, \; a''a^2, \; \ldots, \; a''a^{r-1}.$$

Nous démontrerons facilement que les nombres de cette suite sont incongrus entre eux et incongrus aussi à tous les nombres des suites (I) et (II); il en résulte que l'on a, ou bien

$$p-1 = 3r,$$

ou bien

$$p-1 > 3r.$$

On voit qu'en continuant ce raisonnement on arrive nécessairement à la conclusion que $p-1$ est un multiple de r; il en résulte

$$a^{p-1} \equiv 1 \qquad (\text{mod. } p),$$

c'est-à-dire précisément le théorème de Fermat.

25. On peut se demander si, étant donné un diviseur arbitraire de $p-1$ il y a des nombres qui lui appartiennent et combien parmi eux sont incongrus; si nous désignons par $\psi(d)$ le nombre des entiers incongrus qui appartiennent au diviseur d de $p-1$, il est clair que l'on a

$$\Sigma\psi(d) = p-1$$

puisque chacun des $p-1$ nombres

$$1, \; 2, \; 3, \; \ldots, \; p-1$$

appartient à un diviseur d de $p-1$ et à un seul.

D'après une remarque que nous avons faite (§ 13) on est amené à en conclure l'égalité

$$\psi(d) = \varphi(d),$$

en désignant par $\varphi(d)$ le nombre des entiers premiers avec d et non

supérieurs à d. La conclusion, quoique vraie, n'est pas rigoureuse, parce que l'égalité $\Sigma\psi(d) = m$, où la sommation est étendue à tous les diviseurs de m, n'est pas démontrée quel que soit m; en étudiant de plus près la démonstration du § 11, on peut rendre la conclusion rigoureuse; mais nous préférons reproduire le raisonnement remarquable par lequel *Gauss* a établi cette importante proposition.

Supposons qu'il y ait un nombre a qui appartienne à l'exposant d; cherchons s'il y a d'autres nombres appartenant à l'exposant d; s'il en existe effectivement, ils seront racines de la congruence

$$x^d - 1 \equiv 0 \qquad (\text{mod. } p).$$

Or cette congruence a visiblement pour racines les nombres

$$1, a, a^2, \ldots, a^{d-1}$$

et comme ces nombres sont incongrus, ce sont là *toutes ses racines* ($x^d - 1$ divisant $x^{p-1} - 1$, on savait *a priori* que cette congruence avait d racines incongrues). Cherchons à quel exposant appartient une racine quelconque a^α; soit r le plus petit nombre tel que l'on ait

$$(a^\alpha)^r = a^{\alpha r} \equiv 1 \qquad (\text{mod. } p);$$

a appartenant à l'exposant d; αr doit être divisible par d; si δ est le plus grand commun diviseur entre α et d, la plus petite valeur de r telle que αr soit divisible par d est manifestement $\frac{d}{\delta}$; la racine a^α appartient donc à l'exposant $\frac{d}{\delta}\cdot$ Pour que a^α appartienne à l'exposant d, il faut et il suffit que $\delta = 1$, c'est-à-dire que α soit premier avec d; donc s'il existe un nombre a appartenant à l'exposant d, il y en a $\varphi(d)$, $\varphi(d)$ ayant la signification rappelée plus haut. En désignant par $\psi(d)$ le nombre des racines appartenant à un exposant quelconque d, on a, par suite,

ou bien $$\psi(d) = 0,$$

ou bien $$\psi(d) = \varphi(d).$$

Mais

$$\Sigma\psi(d) = p - 1 = \Sigma\varphi(d).$$

On a donc *toujours*

$$\psi(d) = \varphi(d).$$

En particulier, il y a $\varphi(p-1)$ nombres qui appartiennent à l'exposant $p-1$. Ils sont dits *racines primitives* du nombre p.

On dit aussi quelquefois que les nombres qui appartiennent à l'exposant d, sont les *racines primitives de la congruence*

$$x^d - 1 \equiv 0 \pmod{p};$$

mais lorsqu'on parle simplement de *racines primitives*, il faut entendre les nombres qui appartiennent à l'exposant $p-1$.

La propriété fondamentale des racines primitives est que leurs puissances engendrent un système complet de restes (mod. p), sauf zéro. Si g désigne une racine primitive, les résidus minima des nombres

$$g^0 = 1, \quad g, \; g^2, \ldots, \quad g^{p-2}$$

sont, dans un certain ordre, les nombres

$$1, \; 2, \; 3, \; \ldots, \; p-1.$$

Si on considère un nombre quelconque premier avec p, il existe une puissance de g (et par suite une infinité) congrue à ce nombre. *L'exposant de la puissance à laquelle il faut élever g pour avoir un résultat congru au nombre a s'appelle l'indice de a par rapport à la racine primitive g.* On le désigne par la notation : ind. a. On a donc, par définition,

$$g^{\text{ind}.a} \equiv a \pmod{p}.$$

Tout nombre (non nul mod. p) a une infinité d'indices, congrus entre eux *suivant le module* $p-1$. Lorsque nous dirons que deux *indices* sont congrus ou égaux, cela signifiera donc toujours : *congrus suivant le module* $p-1$. Avec cette convention, les propriétés des indices s'énoncent exactement de la même manière que celles des logarithmes. La propriété fondamentale est, comme pour ces derniers, que *l'indice d'un produit est égal à la somme des indices de ses facteurs* et on en déduit les mêmes conséquences.

Par exemple lorsqu'on change la *base* des indices, c'est-à-dire lorsqu'on remplace la racine primitive g par une autre γ, on passe d'un système d'indices à un autre comme d'un système de logarithmes à un autre ; si nous convenons de désigner par la notation I. a les indices dans le système de base g, en employant la notation habituelle dans le système de base γ, nous avons

$$\gamma = g^{\text{I}.\gamma}$$

et par suite, a désignant un nombre quelconque,

$$a = \gamma^{\text{ind}.a} = g^{(\text{I}.\gamma)(\text{ind}.a)},$$

c'est-à-dire

$$(\mathrm{l}.\gamma)(\mathrm{ind}.a) \equiv \mathrm{l}.a \qquad (\mathrm{mod.}\ p-1)$$

ou, en employant la notation de Gauss,

$$\mathrm{ind.}\ a \equiv \frac{\mathrm{l}.a}{\mathrm{l}.\gamma} \qquad (\mathrm{mod.}\ p-1).$$

En particulier,

$$\mathrm{ind.}\ g \equiv \frac{1}{\mathrm{l}.\gamma} \qquad (\mathrm{mod.}\ p-1).$$

26. On peut à l'aide d'une *table d'indices* résoudre les congruences du premier degré ; car, de la congruence

$$ax \equiv b \qquad (\mathrm{mod.}\ p),$$

on tire

$$\mathrm{ind.}\ x \equiv \mathrm{ind.}\ b. - \mathrm{ind.}\ a \qquad (\mathrm{mod.}\ p-1).$$

Considérons par exemple le nombre 13, pour lequel 2 est racine primitive ; on forme facilement la table d'indices suivante :

ind. x	0	1	2	3	4	5	6	7	8	9	10	11	12
x	1	2	4	8	3	6	12	11	9	5	10	7	1

(On obtient chaque nombre de la seconde ligne en multipliant le précédent par 2 et prenant le résidu minimum par rapport à 13). On en conclut la seconde table :

x	1	2	3	4	5	6	7	8	9	10	11	12
ind. x	0	1	4	2	9	5	11	3	8	10	7	6

Proposons-nous, par exemple, de résoudre la congruence

$$7x \equiv 5 \qquad (\mathrm{mod.}\ 13);$$

nous en concluons, en nous servant de la seconde table,

$$\mathrm{ind.}\ x \equiv \mathrm{ind.}\ 5 - \mathrm{ind.}\ 7 \equiv 9 - 11 \equiv 10 \qquad (\mathrm{mod.}\ 12),$$

et par suite, à l'aide de la première table,

$$x \equiv 10 \qquad (\mathrm{mod.}\ 13).$$

De même, la congruence

$$8x \equiv 3 \qquad (\mathrm{mod.}\ 13)$$

donne

$$\text{ind. } x \equiv \text{ind. } 3 - \text{ind. } 8 \equiv 4 - 3 \equiv 1 \pmod{12}$$

$$x \equiv 2 \pmod{13}.$$

Ici l'usage des indices n'est que commode ; il est des cas où il est presque indispensable. Aussi est-il bon d'être en mesure de former une table d'indices ; pour cela il est nécessaire de connaître, pour chaque nombre premier, une racine primitive. On ne connaît pas de méthode simple pour rechercher les racines primitives ; mais voici un tableau faisant connaître, pour chaque nombre premier inférieur à 100, la plus petite racine primitive :

3	5	7	11	13	17	19	23	29	31	37	41
2	2	3	2	2	3	2	5	2	3	2	6
43	47	53	59	61	67	71	73	79	83	89	97
3	5	2	2	2	2	7	5	3	2	3	5

Il est facile, connaissant une racine primitive, de les avoir toutes ; et plus généralement de trouver tous les nombres appartenant à un exposant donné. En effet, soit g une racine primitive ; cherchons à quel exposant appartient g^α ; soit r le plus petit nombre tel que l'on ait

$$(g^\alpha)^r = g^{\alpha r} \equiv 1 \pmod{p};$$

r est le plus petit nombre tel que l'on ait

$$\alpha r \equiv 0 \pmod{p-1}.$$

Donc si δ désigne le plus grand commun diviseur de α et de $p-1$, on a

$$r = \frac{p-1}{\delta}.$$

(Nous avons déjà fait un calcul identique dans la démonstration de Gauss reproduite plus haut). On aura donc tous les nombres appartenant à l'exposant r, en élevant g à une puissance dont l'exposant α soit tel, que le plus grand commun diviseur de α et de $p-1$ soit $\delta = \frac{p-1}{r}$. On voit que si on connaît l'indice α d'un nombre, on peut déterminer facilement à quel exposant il appartient.

II. — Extension aux imaginaires de Galois.

27. Avant d'aborder d'autres applications de la théorie des indices, nous allons montrer qu'elle s'étend immédiatement aux imaginaires de Galois. Si nous supposons que le premier membre $f(i)$ de la congruence irréductible fondamentale $f(i)$ soit de degré n, il y a $p^n - 1$ imaginaires de Galois incongrues entre elles et à zéro. On verra par un raisonnement identique à celui que nous avons fait que chacun de ces *nombres* (réels ou imaginaires) *appartient* à un exposant qui est un diviseur de $p^n - 1$; et que si r désigne un diviseur quelconque de $p^n - 1$ il y a précisément $\varphi(r)$ nombres qui appartiennent à l'exposant r. En particulier, il y a $\varphi(p^n - 1)$ nombres qui appartiennent à l'exposant $p^n - 1$; on peut les appeler racines *primitives pour le module* p *et la fonction irréductible* $f(i)$.

Cette notion va nous permettre d'approfondir un peu plus que nous ne l'avions fait l'étude des racines imaginaires des congruences irréductibles et *aussi d'étudier les rapports entre les imaginaires de Galois qui correspondent à des congruences fondamentales différentes.*

Soit j une imaginaire de Galois :

$$j \equiv \alpha_0 + \alpha_1 i + \ldots + \alpha_{n-1} i^{n-1} \quad [\text{modd. } p, f(i)];$$

nous savons que j est racine d'une certaine congruence irréductible :

$$g(x) \equiv 0 \qquad [\text{modd. } p, f(i)]$$

dont le degré est égal à n ou à un diviseur de n. Il est facile de déterminer ce degré connaissant l'exposant α auquel appartient j. En effet, nous savons que α divise $p^n - 1$; si nous désignons par r le plus petit nombre tel que $p^r - 1$ soit divisible par α, nous aurons

$$j^{p^r} \equiv j \qquad [\text{modd. } p, f(i)],$$

et r sera le plus petit nombre tel que cette congruence ait lieu. Il en résulte que $g(x)$ est de degré r. (On voit que r est un diviseur de n; il serait facile de le montrer directement.) On convient de dire, lorsque r est le plus petit nombre tel que $p^r - 1$ soit divisible par α, que α est un diviseur *propre* de $p^r - 1$. Les racines d'une congruence irréductible quelconque $g(x)$ de degré r appar-

tiennent donc à un même exposant α, diviseur propre de $p^r - 1$ et $x^\alpha - 1$ est divisible par $g(x)$ (mod. p); on peut dire que *la congruence irréductible* $g(x)$ *appartient à l'exposant* α. Le nombre des imaginaires qui appartiennent à l'exposant α est $\varphi(\alpha)$; comme chaque congruence de degré r a r racines, il y a $\frac{\varphi(\alpha)}{r}$ congruences qui appartiennent à l'exposant α (*).

En particulier il y a $\frac{\varphi(p^n - 1)}{n}$ congruences irréductibles de degré n qui appartiennent à l'exposant $p^n - 1$; elles ont pour racines les $\varphi(p^n - 1)$ *racines primitives* (**). Si l'on choisit comme *congruence fondamentale* une de ces congruences que l'on peut appeler *primitives*, i sera une racine primitive et par suite les $p^n - 1$ premières puissances de i constitueront un système complet de nombres incongrus entre eux et à zéro.

Il est facile de trouver l'expression de toutes les racines d'une congruence irréductible quelconque en fonction de l'une d'entre elles. Remarquons d'abord que si une imaginaire j appartient à l'exposant λ, diviseur propre de $p^r - 1$, les r quantités

$$j, j^p, j^{p^2}, \ldots, j^{p^{r-1}}$$

sont distinctes. En effet, si on avait

$$j^{p^\alpha} \equiv j^{p^\beta} \qquad [\text{modd. } p, f(i)]$$

et

$$\alpha < \beta < n,$$

on en conclurait, en élevant les deux membres à la puissance $p^{r-\alpha}$,

$$j^{p^r} \equiv j^{p^{r+\beta-\alpha}} \qquad [\text{modd. } p, f(i)],$$

ou, à cause de

$$j^{p^r} \equiv j \qquad [\text{modd. } p, f(i)],$$

la congruence

$$j \equiv j^{p^{\beta-\alpha}}$$

dans laquelle on aurait

$$0 < \beta - \alpha < r,$$

ce qui est impossible.

(*) Remarquons en passant ce théorème : α étant un diviseur propre de $p^r - 1$, $\varphi(\alpha)$ est divisible par r.

(**) Nous avons ainsi une limite inférieure du nombre des congruences irréductibles de degré n plus facile à calculer que la valeur exacte donnée plus haut. Mais il importe de remarquer que pour trouver cette limite inférieure, nous avons dû supposer l'existence d'*une* congruence irréductible $f(x)$ de degré n; il aurait donc été impossible de s'en servir pour démontrer qu'il existe effectivement des congruences irréductibles de tous les degrés.

Or, nous avons vu que l'on a, quel que soit λ,

$$F(j^{p^\lambda}) \equiv [F(j)]^{p^\lambda} \qquad (\text{mod. } p).$$

On a donc *a fortiori*

$$F(j^{p^\lambda}) \equiv [F(j)]^{p^\lambda} \qquad [\text{modd. } p, f(i)];$$

il en résulte que si la congruence

$$F(x) \equiv 0 \qquad [\text{modd. } p, f(i)]$$

admet la racine j, elle admet aussi pour racine j^{p^λ} *quel que soit* λ. Mais nous venons de voir que si $F(x)$ est de degré r, parmi toutes les quantités j^{p^λ} il y en a précisément r de distinctes; ce sont donc *toutes* les racines de la congruence proposée.

28. Ces préliminaires établis, considérons une congruence irréductible de degré n,

$$g(x) \equiv 0 \qquad [\text{modd. } p, f(i)]$$

(nous supposons toujours que n désigne le degré de $f(i)$). Soit

$$j \equiv \varphi(i) \equiv a_0 + a_1 i + \ldots + a_{n-1} i^{n-1}$$

une racine de la congruence proposée; les $n-1$ autres racines sont

$$j^p, j^{p^2}, \ldots, j^{p^{n-1}}.$$

Or on a

$$j^{p^2} \equiv [\varphi(i)]^{p^2} \equiv \varphi(i^{p^2}) \qquad [\text{modd. } p, f(i)].$$

Les n racines de la congruence

$$f(x) \equiv 0 \qquad [\text{modd. } p, f(i)]$$

sont, d'après ce qui précède,

$$i, i^p, i^{p^2}, \ldots, i^{p^{n-1}};$$

si on les désigne par $i_1, i_2, \ldots, i_n$ et si on désigne également par $j_1, j_2, \ldots, j_n$ les racines de $g(x)$, on voit que l'on a généralement(*)

$$j_\alpha = \varphi(i_\alpha).$$

On en conclut que si l'on désigne par $G(y) = 0$ la transformée *algébrique* de l'équation $f(x) = 0$ par la transformation $y = \varphi(x)$, on a

$$G(y) \equiv A g(y) \qquad (\text{mod. } p).$$

A désignant une constante. En d'autres termes, on passe de la con-

(*) Il aurait été très facile de voir directement que toutes les quantités $\varphi(i_\alpha)$ sont racines de $g(x)$, mais l'analyse précédente est nécessaire pour montrer que ces quantités sont *distinctes*.

gruence fondamentale à une autre congruence irréductible de même degré par une transformation algébrique, et cette transformation donne précisément l'expression des racines de la seconde congruence en fonction de celles de la première.

Il est clair qu'un polynome irréductible (mod. p) est aussi irréductible algébriquement (c'est-à-dire ne peut être décomposé en facteurs rationnels). La transformation

$$y = \varphi(x)$$

transformant le polynome *irréductible* $f(x)$ dans le polynome *irréductible* $G(y)$, on sait qu'il existe une transformation inverse :

$$x = \psi(y)$$

qui transforme $G(y)$ en $f(x)$ et on sait déterminer algébriquement cette transformation. On conclut de ce qui précède que la congruence

$$f(x) \equiv 0 \qquad [\text{modd. } p, g(j)],$$

où nous désignons par j l'imaginaire de Galois fondamentale, admet la racine

$$i = \psi(j).$$

Il est maintenant facile de voir ce qui arrive lorsqu'on remplace $f(x)$ par $g(x)$ comme congruence fondamentale. Nous désignerons par j l'imaginaire de Galois qui est relative à $g(x)$ et nous allons voir que le résultat est fort simple. On doit opérer comme on serait naturellement amené à le faire, *si on admettait* a priori, *que les racines imaginaires des congruences irréductibles ont une existence effective*, c'est-à-dire indépendante du choix de la congruence fondamentale. D'une manière plus précise, si la congruence

$$F(x) \equiv 0 \qquad [\text{modd. } p, f(i)]$$

admet la racine $h(i)$, la congruence

$$F(x) \equiv 0 \qquad [\text{modd. } p, g(j)]$$

admet la racine $h[\psi(j)]$. En effet, $F[h(i)]$ est divisible par $f(i)$ suivant le module p ; donc $F[h(\psi j)]$ est divisible par $f(\psi j)$. Mais d'après la théorie de la transformation, nous savons que $f(\psi y)$ est divisible *algébriquement* par $G(y)$; donc $f(\psi j)$ est divisible par $g(j)$ suivant le module p et par suite $F[h(\psi j)]$ l'est aussi, c'est-à-dire que $h(\psi j)$ est racine de

$$F(x) \equiv 0 \qquad [\text{modd. } p, g(j)].$$

Nous sommes maintenant assurés que l'existence de relations entre les racines de plusieurs congruences irréductibles est indépendante du choix de la *congruence fondamentale*. Ce choix n'a donc pas l'importance excessive qu'on aurait pu lui attribuer tout d'abord ; c'est simplement un *moyen* pour étudier certaines relations.

On a remarqué, dans le chapitre précédent, qu'il est impossible d'exprimer les racines d'une congruence irréductible, de degré r, au moyen de l'imaginaire définie par une congruence fondamentale de degré n, lorsque n n'est pas un multiple de r. Il en résulte que la relation entre les imaginaires de Galois correspondant à deux congruences fondamentales de degrés différents n'est simple que si le degré de l'une est un multiple du degré de l'autre.

On peut, lorsqu'on a des congruences de degrés différents quelconques, considérer une congruence irréductible dont le degré est le plus petit multiple commun des degrés des congruences proposées. Mais nous ne voulons pas trop nous étendre sur ce sujet. Bornons-nous à énoncer le résultat suivant, relatif au cas où le degré n de la congruence fondamentale primitive $f(i)$ est un multiple du degré r de la congruence fondamentale nouvelle $g(j)$. Si alors

$$j \equiv \varphi(i) \qquad [\text{modd. } p,\ f(i)]$$

est une racine de la congruence

$$g(x) \equiv 0 \qquad [\text{modd. } p,\ f(i)],$$

la transformée *algébrique* de l'équation $f(x) = 0$ par la transformation $y = \varphi(x)$ étant $G(y) = 0$, on a

$$G(y) \equiv [g(y)]^{\rho} \qquad (\text{mod. } p),$$

en posant $n = r\rho$.

Il résulte de là que si l'on effectue sur une équation

$$f(x) = 0$$

dont le premier membre est irréductible (mod. p) une transformation rationnelle quelconque :

$$y = \varphi(x),$$

le résultat est irréductible (mod. p) ou congru à une puissance d'un polynome irréductible.

On verrait facilement que l'on passerait du cas où la congruence irréductible est $g(j)$ au cas où elle est $f(i)$ par une simple transformation entière $[j = \varphi(i)]$, mais la réciproque n'est évidemment pas vraie.

III. — Applications. Modules composés.

29. Nous allons maintenant considérer exclusivement les nombres réels, sans indiquer l'extension aux imaginaires de Galois des applications que nous allons faire.

Les considérations que nous avons développées constituent une étude de la congruence

$$x^n \equiv 1 \pmod{p}.$$

Nous savons en effet résoudre cette congruence ; si δ désigne le plus grand commun diviseur de n et de $p-1$ et g une racine primitive pour le nombre premier p, ses racines sont visiblement

$$g^{\frac{p-1}{\delta}}, \quad g^{2\frac{p-1}{\delta}}, \quad g^{3\frac{p-1}{\delta}}, \quad \ldots\ldots, \quad g^{(\delta-1)\frac{p-1}{\delta}};$$

et leur nombre est δ.

Proposons-nous de résoudre la congruence binome plus générale (*)

$$x^n \equiv \mathrm{D} \pmod{p}.$$

D'après les propriétés des indices, nous devons avoir

$$n \text{ ind. } x \equiv \text{ind. D} \pmod{p-1}.$$

C'est une congruence du premier degré en ind. x.

Si n est premier avec $p-1$, cette congruence admettra une solution et une seule et il en sera de même de la congruence proposée.

Si n n'est pas premier avec $p-1$, désignons par δ leur plus grand commun diviseur. La congruence est impossible si δ ne divise pas ind. D; si δ divise ind. D, elle admet δ solutions incongrues ; il en est de même de la congruence proposée. Donc *la condition nécessaire et suffisante pour que la congruence*

$$x^n \equiv \mathrm{D} \pmod{p}$$

soit possible est que ind. D *soit divisible par le plus grand commun diviseur* δ *de* n *et de* $p-1$; *la congruence admet alors* δ *solutions.*

Il est manifeste que le résultat doit être indépendant de la racine primitive choisie comme base des indices. Il est donc naturel de

(*) La congruence

$$ax^n \equiv b \pmod{p}$$

se ramène à celle que nous considérons dans le texte en posant

$$\mathrm{D} \equiv \frac{b}{a} \pmod{p}.$$

chercher à mettre la condition de possibilité sous une forme où n'apparaisse plus cette racine primitive. Posons

$$\text{ind. } D = d$$

et désignons par g la base des indices ; nous aurons

$$g^d \equiv D \qquad (\text{mod. } p).$$

Élevons les deux membres à la puissance *entière* $\frac{p-1}{\delta}$; il vient

$$g^{d.\frac{p-1}{\delta}} = D^{\frac{p-1}{\delta}}.$$

Si δ divise d, $\frac{d(p-1)}{\delta}$ sera divisible par $p-1$ et le premier membre sera congru à 1 ; il est donc nécessaire que l'on ait

$$D^{\frac{p-1}{\delta}} \equiv 1 \qquad (\text{mod. } p).$$

Cette condition est d'ailleurs suffisante, car si elle est vérifiée, on a

$$\frac{p-1}{\delta}\,\text{ind. } D \equiv 0 \qquad (\text{mod. } p-1),$$

c'est-à-dire que ind. D est divisible par δ.

Donc *la condition nécessaire et suffisante pour que la congruence*

$$x^n \equiv D \qquad (\text{mod. } p)$$

soit possible, est que l'on ait

$$D^{\frac{p-1}{\delta}} \equiv 1 \qquad (\text{mod. } p).$$

Reprenons la question dans le cas où n divise $p-1$. Soit

$$p-1 = nq.$$

Il est clair que le procédé le plus élémentaire pour résoudre la congruence

$$x^n \equiv D \qquad (\text{mod. } p)$$

consiste à former successivement les $n^{\text{ièmes}}$ puissances de $p-1$ nombres incongrus entre eux et à zéro, de prendre les résidus minima de ces puissances et d'examiner si l'un de ces résidus est égal à D (nous supposons D compris entre 0 et p). C'est ce procédé élémentaire qui va nous permettre l'étude de la question en ayant soin de prendre pour les $p-1$ nombres incongrus dont nous venons de parler, les $p-1$ premières puissances d'une même racine primitive :

$$g,\ g^2,\ \ldots,\ g^{p-2},\ g^{p-1} ;$$

leurs $n^{\text{ièmes}}$ puissances sont

$$g^n,\ g^{2n},\ \ldots,\ g^{(p-2)n},\ g^{(p-1)n},$$

et nous pouvons visiblement les écrire de la manière suivante :

$$\begin{array}{llcl} g^n & g^{2n} & \ldots\ldots\ldots\ldots & g^{qn} \\ g^{(q+1)n} & g^{(q+2)n} & \ldots\ldots\ldots\ldots & g^{2qn} \\ \ldots & \ldots & \ldots\ldots\ldots\ldots & \ldots \\ \ldots & \ldots & \ldots\ldots\ldots\ldots & \ldots \\ g^{[(n-1)q+1]n} & g^{[(n-1)q+2]n} & \ldots\ldots\ldots\ldots & g^{nqn}. \end{array}$$

Si nous remarquons que l'on a

$$g^{qn} = g^{p-1} \equiv 1 \qquad (\text{mod. } p),$$

l'on voit que les nombres inscrits dans une même colonne ont un même résidu minimum ; il y a donc seulement q résidus minima différents, ce sont les résidus des puissances

$$g^n,\ g^{2n},\ \ldots,\ g^{qn}$$

(dont la dernière est congrue à l'unité puisque qn est égal à $p-1$) ; ces résidus sont d'ailleurs tous différents et l'on aperçoit immédiatement que ce sont les q racines de la congruence

$$x^q \equiv 1 \qquad (\text{mod. } p).$$

Donc, pour que D se trouve parmi ces nombres, il faut que l'on ait

$$D^q = D^{\frac{p-1}{n}} \equiv 1 \qquad (\text{mod. } p);$$

c'est la condition déjà trouvée.

30. Mais le tableau que nous venons de faire nous permet d'approfondir davantage cette question et de partager en classes les nombres D pour lesquels la congruence

$$x^n \equiv D \qquad (\text{mod. } p)$$

n'est pas possible. Nous avons posé $p-1 = nq$; il est clair qu'en appliquant au nombre q ce que nous venons de dire pour le nombre n, c'est-à-dire en élevant à la $q^{\text{ième}}$ puissance tous les nombres incongrus entre eux et à zéro suivant le module p (c'est-à-dire les nombres $g, g^2, \ldots, g^{p-1}$), nous obtiendrons seulement n résultats incongrus

$$g^q,\ g^{2q},\ \ldots,\ g^{nq}$$

ou, en posant $g^q \equiv f$:

$$f,\ f^2,\ \ldots,\ f^n \equiv 1.$$

Donc, f est une racine primitive de la congruence

$$x^n \equiv 1 \pmod{p}.$$

Cela posé, les $p-1$ nombres considérés se partagent naturellement en n classes, la $k^{ième}$ classe comprenant les nombres D pour lesquels on a

$$D^q \equiv f^k \pmod{p}.$$

En particulier, les nombres de la $n^{ième}$ classe sont ceux pour lesquels on a

$$D^q \equiv f^n \equiv 1 \pmod{p},$$

c'est-à-dire pour lesquels la congruence $a^n \equiv D$ est possible ; ils sont dits : *résidus de $n^{ièmes}$ puissances.*

Il est clair que si l'on a

$$D^q \equiv f^k \pmod{p},$$

$$D'^q \equiv f^{k'} \pmod{p},$$

il en résulte

$$(DD')^q \equiv f^{k+k'} \pmod{p},$$

et comme f^n est congru à l'unité on peut si l'exposant $k+k'$ dépasse n, le remplacer par $k+k'-n$. On peut donc dire que le numéro de la classe à laquelle appartient un produit de plusieurs facteurs est congru (mod. n) à la somme des numéros des classes de ces facteurs. C'est cette proposition qui fait l'importance de la division en classes.

Cette division en classes a été indiquée pour la première fois par Gauss dans le cas de $n = 4$ (on a alors $p = 4q+1$). Les nombres D pour lesquels la congruence est possible s'appellent *résidus biquadratiques* du nombre p. L'analyse faite par Gauss, au sujet des résidus biquadratiques (Werke, Band II) s'étend d'elle-même au cas où n dépasse 4 ; tandis que si l'on étudiait seulement les *résidus quadratiques* ($n = 2$) la généralisation des propriétés des classes n'apparaîtrait pas d'une manière aussi évidente.

Dans le cas où $n = 4$ ($p = 4q+1$), on doit désigner par f une racine primitive de la congruence

(1) $$x^4 \equiv 1 \pmod{p}.$$

On a alors

$$f^2 \equiv -1 \pmod{p},$$

car d'après la définition de f, on a

$$(f^2+1)(f^2-1)\equiv 0 \quad (\text{mod. } p),$$

et le second facteur ne peut pas être nul, sinon f ne serait pas racine *primitive* de la congruence (1). On a donc

$$f^2 \equiv -1 \quad (\text{mod. } p),$$

$$f^3 \equiv -f \quad (\text{mod. } p).$$

On en conclut que si l'on a :

$D^q \equiv +f$ (mod. p), D appartient à la 1re classe;
$D^q \equiv -1$ » , » 2e » ;
$D^q \equiv -f$ » , » 3e » ;
$D^q \equiv +1$ » , » 4e » .

Les nombres de la quatrième classe sont les résidus biquadratiques de p. Nous avons posé $q=\frac{p-1}{4}$.

Supposons par exemple $p=13$; on a alors $q=3$ et on peut prendre $f=5$. (On pourrait aussi prendre $f=-5\equiv 8$ (mod. 13). Il en résulterait un échange de la première classe avec la troisième, sans importance pour notre but; il en est de même dans le cas général).

Nous avons, en prenant $f=5$:

$$2^3 \equiv 8 \equiv -f \quad (\text{mod. } 13).$$

Donc 2 est rangé dans la troisième classe ; $8=2^3$ sera rangé dans la classe dont le rang est congru à 3×3 (mod. 4), c'est-à-dire dans la première classe ; 8 est donc un résidu biquadratique de 13.

Nous ne nous étendons pas sur cet exemple et nous n'examinons pas ici le cas fort important de $n=2$, qui fera l'objet du chapitre suivant.

31. Pour achever l'étude des congruences binomes, il nous resterait à traiter directement le cas des modules composés. C'est ce que nous ferons plus loin pour les congruences du second degré. Ici, nous allons nous borner à énoncer les résultats principaux dans le cas général ; il est facile de les vérifier.

Supposons d'abord que le module soit une puissance p^α d'un nombre premier impair ; on vérifie alors facilement qu'il existe des

racines primitives, c'est-à-dire des nombres g satisfaisant à la congruence

$$g^{\varphi(p^\alpha)} \equiv 1 \pmod{p^\alpha}$$

(qui exprime le théorème de Fermat généralisé) et ne satisfaisant à aucune congruence de la forme

$$g^r \equiv 1 \pmod{p^\alpha},$$

dans laquelle r est inférieur à $\varphi(p^\alpha)$. D'ailleurs, lorsqu'on a démontré l'existence des racines primitives de proche en proche (c'est-à-dire en supposant leur existence pour le module $p^{\alpha-1}$ afin de la démontrer pour le module p^α), on voit facilement par un raisonnement direct que leur nombre est $\varphi[\varphi(p^\alpha)]$. En élevant une racine primitive aux puissances $1, 2, 3, \ldots, \varphi(p^\alpha)$, on obtient *un système complet de restes premiers avec* p^α, suivant le module p^α. Nous avons déjà remarqué que l'ensemble des nombres premiers avec le module et inférieurs au module, joue souvent, dans le cas d'un module composé, le même rôle que le système complet de restes incongrus à zéro dans le cas du module premier. On obtient toutes les racines primitives en élevant l'une d'elles successivement aux diverses puissances dont l'exposant est premier avec $\varphi(p^\alpha)$.

On voit que l'on peut faire correspondre à l'un quelconque x des $\varphi(p^\alpha)$ nombres inférieurs à p^α et premiers avec p^α l'exposant auquel il faut élever une racine primitive déterminée pour obtenir un nombre congru à $x \pmod{p^\alpha}$. Cet exposant est ce qu'on appellera *l'indice* de x et ces indices ont les mêmes propriétés et par suite les mêmes applications que dans le cas des modules premiers.

Les choses se passent d'une manière toute différente lorsque le module est une puissance de 2. Le cas du module 2 est sans intérêt ; pour le module $2^2 = 4$, le nombre 3 joue le rôle de racine primitive ; car on a $3^2 \equiv 1 \pmod{4}$. Examinons le cas du module $2^3 = 8$. Il est facile de vérifier que le carré de tout nombre impair est de la forme $8n + 1$; il n'y a donc pas de racines primitives pour le module 8 ; car on a $\varphi(8) = 4$ et α étant un nombre quelconque premier avec 8,

$$\alpha^2 \equiv 1 \pmod{8}.$$

Mais on peut remarquer que tout nombre est congru (mod. 8) à l'une des quatre valeurs que prend l'expression $(-1)^\alpha 5^\beta$, lorsque

α et β parcourent séparément un système complet de restes (mod. 2).

Ceci se généralise pour les puissances de 2 supérieures à la troisième ; on a $\varphi(2^n) = 2^{n-1}$ et α étant un nombre impair quelconque,

$$\alpha^{2^{n-2}} \equiv 1 \qquad (\text{mod. } 2^n).$$

De plus, il existe effectivement des nombres impairs tels que leur puissance d'exposant 2^{n-2} soit la première qui soit congrue à 1 (mod. 2^n) ; en particulier le nombre 5 jouit de cette propriété, quel que soit n. Dès lors tout nombre impair est congru (mod. 2^n) à l'une des valeurs de l'expression $(-1)^\alpha 5^\beta$ où α et β parcourent respectivement un système complet de restes, α suivant le module 2 et β suivant le module 2^{n-2}. Les nombres α et β peuvent être appelés *les indices* du nombre $(-1)^\alpha 5^\beta$; ce système de deux indices a des propriétés tout à fait analogues aux indices uniques déjà considérés.

Prenons enfin un nombre composé quelconque : $k = 2^m q^n q'^{n'}$; soient g, g' des racines primitives pour les modules q et q', et N un nombre quelconque ; on aura :

$$N \equiv (-1)^\alpha 5^\beta \qquad (\text{mod. } 2^m),$$
$$N \equiv g^\gamma \qquad (\text{mod. } q^n),$$
$$N \equiv g'^{\gamma'} \qquad (\text{mod. } q^{n'}),$$

les nombres α, β, γ, γ' étant complètement déterminés, *suivant les modules respectifs* 2, 2^{n-2}, $\varphi(q^n)$, $\varphi(q^{n'})$. Ces nombres α, β, γ, γ' seront appelés *les indices* de N ; deux nombres N sont congrus (mod. k) lorsque leurs indices sont respectivement congrus (suivant les modules déjà indiqués). Les indices d'un produit sont égaux (ou congrus) à la somme des indices correspondants des facteurs, etc...

Pour plus de détails sur cette théorie nous renverrons à la théorie des nombres de Lejeune Dirichlet (supplément V).

CHAPITRE IV

RÉSIDUS QUADRATIQUES. — LOI DE RÉCIPROCITÉ

I. — Congruences du second degré.

32. Nous allons nous occuper, dans ce chapitre, des congruences du second degré et particulièrement de celles qui ont la forme binome. Cette étude nous conduira à la notion très importante des *résidus quadratiques*, dont la théorie a pour fondement la *loi de réciprocité* découverte par *Euler* et *Legendre*. Les théories générales développées dans les deux chapitres précédents pourraient trouver une application naturelle dans l'étude que nous allons faire ; mais, à cause de l'importance très grande de cette étude, il nous paraît préférable d'opérer autrement.

Nous allons nous attacher à développer la théorie des résidus quadratiques en elle-même, c'est-à-dire en supposant connues le moins de choses qu'il sera possible. On apercevra immédiatement que certaines des propositions auxquelles nous parviendrons ainsi ne sont que des cas particuliers de théorèmes plus généraux établis précédemment ; mais nous ne supposerons pas connus ces théorèmes, de sorte que la lecture de ce qui va suivre peut succéder immédiatement à celle du premier chapitre de cet ouvrage.

La congruence générale du second degré

$$ax^2 + bx + c \equiv 0 \pmod{m}$$

se ramène immédiatement à la suivante :

$$(2ax + b)^2 \equiv b^2 - 4ac \pmod{4am},$$

que l'on peut écrire

$$y^2 \equiv D \pmod{k}.$$

en posant :

$$2ax + b = y,$$
$$b^2 - 4ac = D,$$
$$4am = k.$$

Une discussion facile permet de voir dans chaque cas particulier si, réciproquement, à une solution de cette seconde congruence correspond une solution de la première.

33. Nous pouvons donc nous borner à étudier la congruence binome, que nous écrirons

$$x^2 \equiv D \pmod{m}.$$

Soit

$$m = 2^\alpha p^\beta q^\gamma r^\delta \ldots,$$

$2, p, q, r, \ldots$ étant les facteurs premiers *distincts* de m (nous verrons bientôt pourquoi il y a lieu de distinguer 2 des nombres premiers impairs). Nous savons qu'à tout système de solutions des congruences

$$x^2 \equiv D \pmod{2^\alpha},$$
$$x^2 \equiv D \pmod{p^\beta},$$
$$x^2 \equiv D \pmod{q^\gamma},$$
$$x^2 \equiv D \pmod{r^\delta}$$
$$\ldots \quad \ldots\ldots$$

correspond une solution de la congruence proposée, et réciproquement. Pour que la congruence proposée soit possible, il est donc nécessaire et suffisant que chacune de ces dernières le soit, et le nombre des solutions de la proposée est alors évidemment égal au produit des nombres qui expriment combien chacune d'elles a de solutions distinctes.

Par exemple la congruence

$$x^2 \equiv 13 \pmod{36}$$

se ramène aux congruences

$$x^2 \equiv 13 \equiv 1 \pmod{4},$$
$$x^2 \equiv 13 \equiv 4 \pmod{9}.$$

La première a les solutions distinctes

$$\left\{\begin{array}{l} x \equiv 1 \\ x \equiv 3 \end{array}\right. \pmod{4};$$

la seconde :

$$\left\{\begin{array}{l} x \equiv 2 \\ x \equiv 7 \end{array}\right. \pmod{9},$$

comme on s'en assure aisément.

En combinant de toutes les manières possibles une solution de la

première avec une solution de la seconde, on obtient les *quatre* solutions distinctes de la proposée :

$$\left.\begin{array}{l} x \equiv 29 \\ x \equiv 25 \\ x \equiv 11 \\ x \equiv 7 \end{array}\right\} \text{(mod. 36), correspondant à :} \left\{\begin{array}{l} 1 \text{ et } 2 \\ 1 \text{ et } 7 \\ 3 \text{ et } 2 \\ 3 \text{ et } 7. \end{array}\right.$$

Nous allons voir que la congruence binome, *lorsqu'elle est possible*, admet *deux* solutions distinctes lorsque le module est un nombre premier impair, *une* seule lorsque le module est égal à 2, *deux* lorsque le module est égal à 4, *quatre* lorsque le module est une puissance de 2 divisible par 8. Il en résulte que le nombre $\psi(m)$ des solutions de la congruence, dans le cas d'un module quelconque m, est donné par la formule

$$\psi(m) = 2^{\lambda+\eta},$$

λ désignant le nombre des *facteurs premiers impairs distincts* de m, et η étant égal à *zéro* si m n'est pas divisible par 4, à *un* si m est divisible par 4 et non par 8 et à *deux* si m est divisible par 8. Nous avons déjà fait usage de cette formule ; pour qu'elle soit démontrée, il nous reste à faire voir l'exactitude des propositions énoncées dans le cas où le module est une puissance d'un nombre premier.

Nous supposons bien entendu que D est premier avec m, c'est-à-dire n'est divisible par aucun des facteurs premiers qui entrent dans m ; c'est d'ailleurs dans ce cas seulement que nous avons fait usage de la formule précédente. Elle ne serait pas exacte dans le cas général où m ne serait pas premier avec D (*).

(*) Si le plus grand commun diviseur de m et de D est de la forme ab^2, le nombre a ne renfermant aucun facteur premier élevé à une puissance supérieure à la première, on constate aisément que x est nécessairement divisible par ab ; en posant $x = aby$, on est ramené à la congruence

$$ab^2\left(ay - \frac{D}{ab^2}\right) \equiv 0 \pmod{m}$$

et par suite, à la congruence

$$ay - D' \equiv 0 \pmod{m'},$$

dans laquelle D' et m' sont premiers entre eux $\left(D' = \frac{D}{ab^2} \text{ et } m' = \frac{m}{ab^2}\right)$. A chaque solution de cette congruence correspondent b solutions distinctes de la proposée.

34. Considérons donc le cas où le module est une puissance d'un nombre premier, que nous supposerons d'abord impair. Pour que la congruence

$$x^2 \equiv D \qquad (\text{mod. } p^\alpha)$$

soit possible, il faut d'abord qu'il en soit ainsi de la congruence

$$x^2 \equiv D \qquad (\text{mod. } p).$$

Lorsque cette dernière congruence est possible, on dit que D est *résidu quadratique de p;* nous verrons plus loin comment on le reconnait ; ici nous allons chercher le nombre des solutions, dans le cas où la congruence est possible. Soit x_0 une solution ; on a

$$D \equiv x_0^2 \qquad (\text{mod. } p)$$

et la congruence proposée peut s'écrire

$$x^2 - x_0^2 \equiv 0 \qquad (\text{mod. } p)$$

ou

$$(x - x_0)(x + x_0) \equiv 0 \qquad (\text{mod. } p).$$

Pour que ce produit de facteurs soit divisible par le nombre premier p, il faut et il suffit que l'un des facteurs soit divisible par p, c'est-à-dire que l'on ait :

ou bien $$x \equiv x_0 \qquad (\text{mod. } p),$$

ou bien $$x \equiv p - x_0 \qquad (\text{mod. } p).$$

La congruence admet donc deux solutions, qui sont distinctes car $2x_0$ ne peut pas être divisible par p, puisque D ne l'est pas et que p est supposé impair ; *on n'a donc pas*

$$x_0 \equiv p - x_0 \qquad (\text{mod. } p),$$

c'est-à-dire $$2x_0 \equiv 0 \qquad (\text{mod. } p).$$

Montrons maintenant que, lorsque D est *résidu quadratique de p*, la congruence

$$x^2 \equiv D \qquad (\text{mod. } p^\alpha)$$

admet deux solutions et deux seulement.

Nous venons de voir que cette proposition est exacte pour $\alpha = 1$; il suffit donc de faire voir que si elle est vraie pour une valeur de α, elle subsiste lorsqu'on augmente cet exposant d'une unité. Soit y une solution de la congruence

$$y^2 \equiv D \qquad (\text{mod. } p^\alpha);$$

nous allons montrer qu'on peut en déduire une solution de la congruence

$$x^2 \equiv D \qquad (\text{mod. } p^{\alpha+1}).$$

Pour cela posons

$$x = y + \lambda p^{\alpha}.$$

Il vient

$$x^2 - \mathrm{D} = y^2 - \mathrm{D} + 2\lambda y p^{\alpha} + \lambda^2 p^{2\alpha} \equiv 0 \pmod{p^{\alpha+1}}.$$

Or, par hypothèse, on a

$$y^2 - \mathrm{D} = \mathrm{M}p^{\alpha};$$

il en résulte donc

$$p^{\alpha}(\mathrm{M} + 2\lambda y + \lambda^2 p^{\alpha}) \equiv 0 \pmod{p^{\alpha+1}},$$

c'est-à-dire

$$\mathrm{M} + 2\lambda y \equiv 0 \pmod{p};$$

$2y$ étant premier avec p, cette congruence détermine λ : on en tire

$$\lambda \equiv \lambda_0 \pmod{p}$$

et par suite

$$x \equiv y + \lambda_0 p^{\alpha} \pmod{p^{\alpha+1}}.$$

On voit ainsi qu'à une solution y correspond une solution x et *une seule ;* il est d'ailleurs aisé de voir directement que la congruence

$$x^2 \equiv \mathrm{D} \pmod{p^{\alpha}}$$

ne peut avoir que deux solutions lorsque D n'est pas divisible par p. En effet, x_0 désignant une solution, x_0 n'est pas divisible par p ; or on doit avoir

$$(x - x_0)(x + x_0) \equiv 0 \pmod{p^{\alpha}};$$

$2x_0$ n'étant pas divisible par p, les deux facteurs ne peuvent pas être divisibles par p ; l'un des deux est donc divisible par p^{α} et l'on a les deux solutions :

$$x \equiv x_0 \pmod{p^{\alpha}},$$
$$x \equiv -x_0 \pmod{p^{\alpha}}.$$

35. Passons maintenant au cas où le module est une puissance de 2 ; nous supposerons, d'après ce qui précède, que D est un nombre impair ; il en résulte que x doit être aussi un nombre impair. Il est clair que la congruence

$$x^2 \equiv \mathrm{D} \pmod{2},$$

où D désigne un nombre impair, admet dans tous les cas la solution unique

$$x \equiv 1 \pmod{2}.$$

Passons à la congruence

$$x^2 \equiv \mathrm{D} \pmod{4}.$$

On vérifie immédiatement que le carré de tout nombre impair est de la forme $4n + 1$; cette congruence n'est donc possible que si l'on a

$$\mathrm{D} \equiv 1 \pmod{4}$$

et elle admet dans ce cas les deux solutions

$$x \equiv 1 \pmod{4},$$
$$x \equiv 3 \pmod{4}.$$

Considérons enfin la congruence

$$x^2 \equiv D \pmod{8}.$$

Tout nombre impair étant de la forme $4k \pm 1$, son carré est de la forme $8n + 1$; la congruence n'est donc possible que si l'on a

$$D \equiv 1 \pmod{8}$$

et elle admet alors les *quatre* solutions

$$\begin{matrix} x \equiv 1 & x \equiv 5 \\ x \equiv 3 & x \equiv 7 \end{matrix} \pmod{8}.$$

Nous pouvons maintenant étudier en général la congruence

$$x^2 \equiv D \pmod{2^{\alpha+1}}.$$

Nous allons montrer que, α étant *plus grand* que 2 (au moins égal à 3), on peut déduire une solution x de cette congruence de toute solution y de la congruence

$$y^2 \equiv D \pmod{2^\alpha}.$$

En effet, posons

$$x = y + \lambda.2^{\alpha-1},$$
$$y^2 - D = M.2^\alpha;$$

il vient

$$x^2 - D = 2^\alpha(M + \lambda y + \lambda^2.2^{\alpha-2}) \equiv 0 \pmod{2^{\alpha+1}}$$

et par suite, $\alpha - 2$ étant positif et non nul,

$$M + \lambda y \equiv 0 \pmod{2},$$

congruence qui donne toujours une valeur de λ, puisque y est impair.

Nous avons ainsi montré que la congruence

$$x^2 \equiv D \pmod{2^\alpha}$$

est possible, lorsque α est plus grand que 3, dans les mêmes cas que lorsque $\alpha = 3$, c'est-à-dire si l'on a

$$D \equiv 1 \pmod{8}.$$

En y regardant de près, notre démonstration prouve même que le nombre des solutions est toujours égal à *quatre*, lorsque la congruence est possible, comme dans le cas du module 8; mais c'est

un point qu'il est aisé de vérifier directement ; soient x et x_0 deux solutions de la congruence

$$x^2 \equiv D \pmod{2^\alpha} ;$$

x et x_0 sont impairs ; $x - x_0$ et $x + x_0$ sont donc tous deux divisibles par 2, mais ne peuvent pas être tous deux divisibles par 4 ; or on a

$$(x - x_0)(x + x_0) \equiv 0 \pmod{2^\alpha} ;$$

deux hypothèses seulement sont donc possibles :

$$\text{I} \begin{cases} x - x_0 \equiv 0 \pmod{2^{\alpha-1}}, \\ x + x_0 \equiv 0 \pmod{2} \end{cases} \qquad \text{II} \begin{cases} x - x_0 \equiv 0 \pmod{2} \\ x + x_0 \equiv 0 \pmod{2^{\alpha-1}} \end{cases}$$

On en déduit les *quatre* solutions distinctes de la congruence :

$$\begin{cases} x \equiv x_0 \\ x \equiv x_0 + 2^{\alpha-1} \end{cases} \pmod{2^\alpha}. \qquad \begin{cases} x \equiv -x_0 \\ x \equiv -x_0 + 2^{\alpha-1} \end{cases} \pmod{2^\alpha}$$

En résumé, *pour que la congruence*

$$x^2 \equiv D \pmod{m}$$

soit possible, il faut et il suffit :

1° *Que* D *soit résidu quadratique de tous les facteurs premiers impairs qui figurent dans* m *;*

2° *Que* D *soit de la forme* $4n + 1$ *si* m *est divisible par* 4, *et de la forme* $8n + 1$ *si* m *est divisible par* 8.

On suppose bien entendu que D et m sont premiers entre eux.

II. — Résidus quadratiques.

36. Il nous faut maintenant étudier la question que nous avons laissée de côté : à quelles conditions un nombre D est-il *résidu quadratique* d'un nombre premier *impair* p ? L'étude de cette question très importante et des problèmes qui s'y rattachent immédiatement fera l'objet de la fin de ce chapitre.

Le procédé à la fois le plus élémentaire et le plus simple pour rechercher les résidus quadratiques d'un nombre premier p, consiste évidemment à former les carrés des nombres $1, 2, 3, \ldots, p-1$ et à prendre leurs résidus minima par rapport à p. Il est clair que tout nombre x étant congru à l'un des nombres $1, 2, 3, \ldots, p-1$, son carré x^2 sera congru au résidu minimum du carré de l'un de

ces nombres. Soit, par exemple, $p = 7$; formons les carrés des 6 premiers nombres,

$$1,\ 4,\ 9,\ 16,\ 25,\ 36\ ;$$

leurs résidus minima (mod. 7) sont

$$1,\ 4,\ 2,\ \ 2,\ 4,\ \ 1.$$

Donc : 1, 2, 4 sont résidus quadratiques de 7 (ou plus simplement *résidus*) ; 3, 5, 6 seront dits *non-résidus*.

On aperçoit sur cet exemple un fait qui est évidemment général ; les résidus minima étant inscrits en ordre sur une même ligne, les termes équidistants des extrêmes sont égaux ; en d'autres termes les carrés des nombres a et $p - a$ ont même résidu. On a en effet

$$a^2 \equiv (p - a)^2 \qquad \text{(mod. } p).$$

Il en résulte que, pour obtenir les résidus de p, il suffit de faire les carrés des nombres 1, 2, 3, ..., $\frac{p-1}{2}$. Le nombre de ces résidus est donc au plus égal à $\frac{p-1}{2}$; il est facile de voir qu'il a précisément cette valeur. En effet, si a et b désignent deux nombres inégaux de la suite 1, 2, 3, ..., $\frac{p-1}{2}$, il est clair que $a - b$ ni $a + b$ ne peuvent être divisibles par p ; on ne peut donc pas avoir

$$a^2 \equiv b^2 \qquad \text{(mod. } p).$$

Il y a donc $\frac{p-1}{2}$ résidus et $\frac{p-1}{2}$ non-résidus.

Il est clair que *le produit de deux résidus* D *et* D' *est un résidu ;* car si l'on a

$$x^2 \equiv \mathrm{D} \qquad \text{(mod. } p),$$

$$x'^2 \equiv \mathrm{D}' \qquad \text{(mod. } p),$$

il en résulte

$$(xx')^2 \equiv \mathrm{DD}' \qquad \text{(mod. } p).$$

Cela posé, considérons un système complet de restes (*) (mod. p); il comprend $\frac{p-1}{2}$ résidus et $\frac{p-1}{2}$ non-résidus. Si on multiplie ce système complet de restes par un résidu R, on obtient encore un système complet de restes, c'est-à-dire $\frac{p-1}{2}$ résidus

(*) Ici et dans la suite, lorsqu'il sera question de système complet de restes, nous excluons le reste *zéro*.

et $\frac{p-1}{2}$ non-résidus. Mais d'après ce qui précède les $\frac{p-1}{2}$ résidus proviennent de la multiplication par R des $\frac{p-1}{2}$ résidus ; donc les $\frac{p-1}{2}$ *non-résidus* proviennent de la multiplication par R des $\frac{p-1}{2}$ *non-résidus*, c'est-à-dire que : *le produit d'un résidu par un non-résidu est un non-résidu.* On démontrerait de même, en considérant le système complet de restes qu'on obtient en multipliant un système complet par un non-résidu, que : *le produit de deux non-résidus est un résidu.* Ces diverses propositions vont d'ailleurs apparaître bientôt comme évidentes.

37. Il est assez naturel de considérer la congruence

$$x^2 \equiv D \pmod{p}$$

comme un cas particulier de la congruence *bilinéaire*

$$yz \equiv D \pmod{p}.$$

Nommons, pour un instant, *nombres associés*, deux nombres y et z qui satisfont simultanément à cette congruence bilinéaire. Il résulte des propriétés des congruences du premier degré que tout nombre a un associé et un seul ; d'ailleurs deux nombres associés ne peuvent être égaux que si D est résidu quadratique de p, et leur valeur commune satisfait à la congruence

$$x^2 \equiv D \pmod{p}.$$

Cette congruence admettant deux solutions x_0 et $p-x_0$, dont le produit est congru à $-x_0^2$ c'est-à-dire à $-D$, il en résulte que : *lorsque* D *est résidu de* p, *il y a deux nombres égaux chacun à son associé ; leur produit est congru à* $-D$.

Il résulte de ce qui précède que :

1° Si D est non-résidu de p, les $p-1$ nombres 1, 2, 3, ..., $p-1$ sont associés deux à deux ; ils forment $\frac{p-1}{2}$ groupes, le produit des nombres de chaque groupe étant congru à D ; on a donc

$$1.2.3 \ldots (p-1) \equiv D^{\frac{p-1}{2}} \pmod{p};$$

2° Si D est résidu de p, il y a deux de ces $p-1$ nombres (x_0 et $p-x_0$) dont le produit est congru à $-D$: les $p-3$

autres sont associés deux à deux comme précédemment et par suite forment $\frac{p-1}{2} - 1$ groupes ; on a donc

$$1.2.3 \ldots (p-1) \equiv -D^{\frac{p-1}{2}} \quad (\text{mod. } p).$$

Si nous remarquons que le nombre 1 est évidemment résidu quadratique, nous retrouvons le théorème de Wilson :

$$1.2.3 \ldots (p-1) \equiv -1 \quad (\text{mod. } p);$$

mais il faut remarquer que cette démonstration ne diffère pas de celle que nous en avons déjà donnée. En faisant usage de ce théorème nous voyons que l'on a

$$D^{\frac{p-1}{2}} \equiv +1 \quad (\text{mod. } p)$$

si D *est résidu* ; et

$$D^{\frac{p-1}{2}} \equiv -1 \quad (\text{mod. } p)$$

si D *est non-résidu.*

Comme tout nombre est nécessairement résidu ou non-résidu et que ces deux congruences sont incompatibles, il en résulte que, réciproquement, *toute solution de la congruence*

$$x^{\frac{p-1}{2}} - 1 \equiv 0 \quad (\text{mod. } p)$$

est un résidu et *toute solution de la congruence*

$$x^{\frac{p-1}{2}} + 1 \equiv 0 \quad (\text{mod. } p)$$

un non-résidu.

Chacune de ces congruences a donc $\frac{p-1}{2}$ solutions ; on a d'ailleurs toujours

$$x^{p-1} \equiv 1 \quad (\text{mod. } p),$$

ce qui est une démonstration *nouvelle* du théorème de Fermat.

On pourrait raisonner de même sur la congruence bilinéaire

$$yz \equiv D \quad (\text{mod. } m)$$

dans le cas où le module m n'est pas premier ; mais il faudrait exclure complètement les nombres D, y et z qui ne seraient pas premiers avec m. On voit alors facilement qu'en désignant par $\varphi(m)$ le nombre des entiers premiers avec m et non supérieurs à m, et par $\psi(m)$ le nombre des solutions qu'admet la congruence

$$x^2 \equiv D \quad (\text{mod. } m)$$

dans les cas où elle est possible, on a :

$$D^{\frac{1}{2}\varphi(m)} \equiv 1 \qquad (\text{mod. } m)$$

lorsque cette congruence est possible, et

$$D^{\frac{1}{2}\varphi(m)} \equiv (-1)^{\frac{1}{2}\psi(m)} \qquad (\text{mod. } m)$$

lorsqu'elle ne l'est pas. Mais ceci ne constitue un théorème vraiment intéressant que lorsque $\psi(m)$ n'est pas divisible par 4, c'est-à-dire lorsque m est égal à une puissance d'un nombre premier impair, au double d'une telle puissance, ou égal à 4. Sinon, on a toujours

$$D^{\frac{1}{2}\varphi(m)} \equiv 1 \qquad (\text{mod. } m)$$

et on ne peut distinguer ainsi si la congruence

$$x^2 \equiv D \qquad (\text{mod. } m)$$

est possible ou non. Aussi nous bornons-nous au cas où le module est un nombre premier.

38. Nous conviendrons de représenter avec *Legendre*, par le symbole

$$\left(\frac{D}{p}\right)$$

l'unité précédée du signe + ou du signe — suivant que D est résidu quadratique ou non-résidu quadratique du nombre premier p.

On a ainsi toujours

$$\left(\frac{D}{p}\right)\left(\frac{D}{p}\right) = 1$$

et, d'après ce qui précède,

$$\left(\frac{D}{p}\right) \equiv D^{\frac{p-1}{2}} \qquad (\text{mod. } p).$$

Il résulte immédiatement de cette congruence l'égalité fondamentale

$$\left(\frac{DD'}{p}\right) = \left(\frac{D}{p}\right)\left(\frac{D'}{p}\right),$$

qui exprime des théorèmes déjà établis directement.

Étant donné un nombre premier p, le problème de rechercher les nombres qui sont résidus et non-résidus ne présente aucune diffi-

culté ; il suffit, comme nous l'avons déjà dit, de former les carrés des termes de la suite $1, 2, 3, \ldots, \frac{p-1}{2}$.

Le problème suivant est beaucoup plus difficile : étant donné un nombre D, trouver les nombres premiers p, tels que D soit résidu quadratique de p. Ce problème s'est présenté depuis longtemps sous une forme à peine différente ; il n'a été résolu complètement que par la belle découverte faite par Euler et par Legendre de la *loi de réciprocité*. Cette loi est ainsi nommée parce qu'elle établit une réciprocité remarquable entre deux nombres premiers quelconques p et q. Si p et q ne sont pas tous deux de la forme $4n+3$, ou bien chacun d'eux est résidu quadratique de l'autre, ou bien chacun d'eux est non-résidu quadratique de l'autre. Si p et q sont tous les deux de la forme $4n+3$, l'un des deux est résidu quadratique de l'autre, lequel est non-résidu du premier. Nous reviendrons d'ailleurs sur cet énoncé pour le généraliser et le traduire analytiquement.

III. — Caractères quadratiques. Symbole de Legendre.

39. Indiquons maintenant comment le problème qui nous occupe s'était posé à *Fermat* et, après lui, à *Euler* et *Lagrange*. Ces géomètres s'étaient proposé de rechercher si la *forme*

$$t^2 - Du^2$$

peut être divisible par un nombre premier p, pour des valeurs entières convenables des variables t et u. Le nombre p est alors dit un diviseur de cette forme. Par exemple, le nombre 7 est un diviseur de la forme

$$x^2 - 2y^2,$$

car pour $x = 3$, $y = 1$, cette forme est divisible par 7.

Le problème de trouver les diviseurs de la forme $t^2 - Du^2$ est complètement équivalent à celui que nous nous proposons ; on suppose, bien entendu, que t et u sont premiers entre eux, car tout diviseur commun à t et u divise la forme. Si p est un diviseur de la forme, il ne peut diviser u ; sinon il diviserait t ; on peut alors trouver un nombre y tel que

$$uy \equiv 1 \qquad (\text{mod. } p).$$

On a alors

$$y^2(t^2 - Du^2) \equiv 0 \qquad (\text{mod. } p),$$

d'où

$$(ty)^2 \equiv Du^2y^2 \equiv D \qquad (\text{mod. } p.),$$

c'est-à-dire que D est résidu quadratique de p ; réciproquement si D est résidu de p, il existe un nombre x tel que

$$x^2 - D \equiv 0 \qquad (\text{mod. } p),$$

et $t^2 - Du^2$ est divisible par p pour $t = x$, $u = 1$.

Le problème que nous nous proposons peut s'énoncer ainsi : D étant un nombre *donné*, trouver un critérium aussi simple que possible pour trouver, *quel que soit* p, la valeur du symbole $\left(\frac{D}{p}\right)$. Il est clair qu'on peut toujours supprimer dans D les puissances paires des nombres premiers qui y figurent : si l'on a

$$D = q^2D',$$

il en résulte

$$\left(\frac{D}{p}\right) = \left(\frac{q}{p}\right)\left(\frac{q}{p}\right)\left(\frac{D'}{p}\right) = \left(\frac{D'}{p}\right).$$

On peut donc supposer que D ne renferme que des facteurs premiers à la première puissance. Nous verrons que lorsque D est un nombre premier, le critérium dont nous venons de parler (qu'on appelle le *caractère quadratique* de D) dépend uniquement du reste de la division de p par 4D ; nous démontrerons par exemple que l'on a

$$\left(\frac{2}{p}\right) = +1$$

si le reste de la division de p par 8 est 1 ou 7, et dans ces cas seulement. De même, pour que

$$\left(\frac{3}{p}\right) = +1,$$

il est nécessaire et suffisant que le reste de la division de p par 12 soit 1 ou 11. On en conclut que le caractère quadratique d'un nombre composé se déduit immédiatement de celui de ses facteurs premiers. Par exemple, en admettant les résultats qui précèdent, on voit que l'on a

$$\left(\frac{6}{p}\right) = +1$$

si le reste de la division de p par 24 est 1, 5, 19 ou 23. Il suffit en effet de former le tableau suivant :

$p \equiv$ à :	$\left(\frac{2}{p}\right)$	$\left(\frac{3}{p}\right)$	$\left(\frac{6}{p}\right)$
1	+1	+1	+1
5	−1	−1	+1
7	+1	−1	−1
11	−1	+1	−1
13	−1	+1	−1
17	+1	−1	−1
19	−1	−1	+1
23	+1	+1	+1

Il nous suffit donc de traiter le problème lorsque D est un nombre premier ; comme nous ne supposons pas que D est positif, nous examinerons successivement les cas suivants :

1° $D = -1$;

2° $D = 2$;

3° D = un nombre premier impair *positif*.

40. Le cas où $D = -1$ se traite immédiatement. D'après une formule déjà établie, on a

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}},$$

c'est-à-dire

$$\left(\frac{-1}{p}\right) = +1$$

si p est de la forme $4n+1$; et

$$\left(\frac{-1}{p}\right) = -1$$

si p est de la forme $4n+3$.

La forme $t^2 + u^2$ *admet donc pour diviseurs les nombres premiers de la forme* $4n+1$ *et ceux-là seulement.* Nous reviendrons sur cette proposition qui est l'une des plus importantes de l'Arithmétique. Elle était connue de Fermat, ainsi d'ailleurs que les résultats que nous allons démontrer pour le nombre 2. Nous allons faire voir que 2 est résidu quadratique des nombres premiers de la forme $8n \pm 1$ et non-résidu de ceux qui ont la forme $8n \pm 3$. Ces propositions seront bientôt établies simultanément par une méthode générale due à Gauss ; mais les démonstrations particulières qui en ont été données sont intéressantes à connaître. Montrons d'abord que 2 est résidu quadratique des nombres premiers p de la forme $8n+1$. Nous nous appuierons pour cela sur une proposition établie dans la théorie générale des congruences (Ch. II) : *toute congruence* (mod. p) *dont le premier membre divise* $x^{p-1} - 1$ *a autant de racines qu'il y a d'unités dans son degré.* Or p étant de la forme $8n+1$, $x^{p-1} - 1$ est divisible par $x^8 - 1$ et par suite, par $x^4 + 1$; la congruence

$$x^4 + 1 \equiv 0 \qquad (\text{mod. } p)$$

a donc quatre racines. Si x désigne l'une d'elles, on a

$$(x^2+1)^2 - 2x^2 \equiv 0 \qquad (\text{mod. } p),$$

ce qui montre que p est un diviseur de la forme $t^2 - 2u^2$, car x^2+1 et x sont premiers entre eux ; donc 2 est résidu de p.

Supposons maintenant que p soit de la forme $8n \pm 3$; il faut montrer que la congruence

$$x^2 - 2 \equiv 0 \qquad (\text{mod. } p)$$

est impossible. On le vérifie sans peine pour $p = 3$. Si donc la proposition n'était pas vraie, il existerait un nombre premier p de la forme $8n \pm 3$, tel que la proposition soit en défaut pour ce nombre, tout en étant vraie pour tous les nombres premiers de même forme inférieurs à p. Il suffit donc de démontrer l'impossibilité d'une telle chose. Si le nombre p existait, la congruence

$$x^2 - 2 \equiv 0 \qquad (\text{mod. } p) \quad p = 8n+3 \quad \text{ou} \quad 8n+5$$

aurait deux solutions inférieures à p ; l'une d'elles serait un nombre impair ; désignons-la par x. Nous allons faire voir que, x étant impair et inférieur à p, $x^2 - 2$ ne pourrait être divisible par p sans être divisible par un nombre premier de même forme et inférieur à p. En effet, le carré de tout nombre impair étant de la forme

$8n+1$, x^2-2 est de la forme $8n-1$ et ne peut par suite être égal à p ; on a donc

$$x^2-2=pf,$$

f étant plus grand que 1. f est d'ailleurs inférieur à p, puisque x est inférieur à p ; tous les facteurs premiers de f sont donc inférieurs à p ; il suffit donc de montrer que l'un au moins de ces facteurs est de la forme $8n+3$ ou $8n+5$. Or, si tous ces facteurs étaient de la forme $8n\pm 1$ (ils sont nécessairement impairs), leur produit f serait de la forme $8n\pm 1$ et le produit pf ne pourrait être de la forme $8n-1$, ce qui est contraire à ce qu'on vient de voir.

Il reste à montrer que 2 est résidu des nombres premiers de la forme $8n+7$; pour ces nombres -1 est non-résidu ; il suffit donc de montrer que -2 est non-résidu. Il résulte de ce qui précède que pour les nombres premiers de la forme $8n+5$, 2 étant non-résidu et -1 résidu, -2 est non-résidu. Nous allons faire voir en même temps que 2 est non-résidu pour les nombres premiers de l'une des formes $8n+5$ ou $8n+7$ (ou si l'on veut $8n-1$ et $8n-3$). Nous avons déjà vu que cette proposition est vraie pour $p=5$; il suffit donc de démontrer la non-existence du plus petit des nombres premiers pour lequel elle ne serait pas vraie. C'est exactement la même marche que nous venons de suivre. Si l'on avait

$$x^2+2=pf,$$

x étant un nombre impair positif inférieur à p et p un nombre de la forme $8n-1$ ou $8n-3$, f admettrait au moins un facteur premier inférieur à p et de l'une de ces deux formes. En effet, si tous les facteurs premiers de f avaient la forme $8n+1$ ou $8n+3$, il en serait de même de f et le produit pf aurait l'une des formes $8n-1$ ou $8n-3$, ce qui est impossible puisque x^2+2 est de la forme $8n+3$.

Les démonstrations précédentes sont dues à Legendre; M. Stieltjes a donné récemment (*) une analyse plus simple que nous allons reproduire.

Soit p un nombre premier impair; considérons la suite des

(*) *Bulletin des sciences mathématiques*, 1884.

$p-1$ nombres

$$1, 2, 3, \ldots\ldots, p-1$$

et supposons que nous écrivions au-dessous de chacun d'eux le signe $+$ ou le signe $-$ suivant qu'il est résidu ou non-résidu quadratique de p. Recherchons le nombre des changements de signe que présente cette suite de signes (A); il y a un changement de signe entre deux nombres k, $k+1$ dans le cas et seulement dans le cas où le nombre r_k, supposé plus petit que p et défini par la relation

$$k+1 \equiv kr_k \qquad (\text{mod. } p)$$

est non-résidu quadratique de p. Mais les nombres

$$r_1, r_2, r_3, \ldots\ldots, r_{p-2}$$

sont visiblement, dans un certain ordre, les nombres

$$2, 3, 4, \ldots\ldots, p-1,$$

car les r sont tous différents et aucun d'eux n'est égal à un. Il y a donc parmi eux $\frac{p-1}{2}$ non-résidus et par suite $\frac{p-1}{2}$ changements de signe dans la suite (A).

Supposons maintenant $p \equiv 1$ (mod. 4). Le nombre des changements de signe de la suite (A) étant pair et le premier nombre 1 de cette suite étant résidu, il s'ensuit que le dernier $p-1$ ou -1 est aussi résidu. Deux nombres k et $p-k$ sont donc en même temps résidus ou non-résidus; si donc on forme la suite analogue à (A),

(B) $$1, 2, 3, \ldots\ldots, \frac{p-1}{2},$$

elle produira un nombre de changements de signe égal à

$$\frac{p-1}{4} = n.$$

Si n est pair, c'est-à-dire $p \equiv 1$ (mod. 8), le dernier nombre $\frac{p-1}{2}$ sera résidu et par suite 2 sera résidu.

Si n est impair, c'est-à-dire $p \equiv 5$ (mod. 8), $\frac{p-1}{2}$ et 2 seront non-résidus.

Soit en second lieu $p \equiv 3$ (mod. 4); le nombre des changements de signe dans la suite (B) sera égal à $\frac{p-3}{4} = n$, car maintenant $\frac{p-1}{2}$ étant impair, -1 est non-résidu.

Si n est pair, c'est-à-dire $p \equiv 3 \pmod{8}$, $\frac{p-1}{2}$ sera résidu et partant 2 sera non-résidu.

Si n est impair, c'est-à-dire $p \equiv 7 \pmod{8}$, $\frac{p-1}{2}$ sera non-résidu et 2 sera résidu.

41. Nous arrivons maintenant au cas où D est un nombre premier impair. La solution du problème est alors donnée par la loi de réciprocité de Legendre (*). Il existe plusieurs démonstrations de cette loi, l'une des plus belles propositions de l'Arithmétique ; Gauss seul en a donné *six;* certaines de ces démonstrations reposent sur des notions très élevées d'analyse mathématique et ne sauraient trouver place ici ; les plus simples reposent sur un lemme dû à Gauss qui est fort intéressant en lui-même. Il fournit en effet une expression analytique du symbole $\left(\frac{D}{p}\right)$ et de plus donne immédiatement le caractère quadratique du nombre 2. Nous allons donc nous occuper d'abord de ce lemme.

Soit D un nombre quelconque non divisible par le nombre premier impair p. Formons les nombres

$$D,\ 2D,\ 3D,\ \ldots\ldots,\ \frac{p-1}{2}D.$$

Tous les termes de cette suite sont incongrus entre eux, c'est-à-dire que la différence de deux termes ne peut pas être divisible par p; la somme de deux termes ne peut pas non plus être divisible par p. Pour chacun des termes, je cherche le *résidu minimum absolu* par rapport à p, c'est-à-dire le reste plus petit en valeur absolue que $\frac{p}{2}$. Soit μ le nombre de ces restes qui sont négatifs. La proposition de Gauss consiste dans l'égalité

$$\left(\frac{D}{p}\right) = (-1)^{\mu}.$$

Pour la démontrer, désignons par

$$\alpha_1,\ \alpha_2,\ \ldots\ldots,\ \alpha_\lambda$$

(*) On donne à cette loi le nom de Legendre parce que, le premier, il l'a énoncée en indiquant son importance. La démonstration qu'il en a donnée présentait d'ailleurs une lacune. Euler avait toutefois énoncé cette loi avant Legendre.

les restes positifs, et par

$$-\beta_1, \quad -\beta_2, \quad \ldots\ldots, \quad -\beta_\mu$$

les restes négatifs. La différence ou la somme de deux quelconques de ces $\lambda + \mu = \frac{p-1}{2}$ restes ne peut pas être divisible par p ; il en résulte que les nombres *positifs*

$$\alpha_1, \ \alpha_2, \ \ldots, \ \alpha_\lambda; \quad \beta_1, \ \beta_2, \ \ldots, \ \beta_\mu$$

sont tous incongrus entre eux et sont par suite dans un certain ordre les nombres

$$1, \ 2, \ 3, \ \ldots\ldots, \frac{p-1}{2}.$$

On a donc

$$\alpha_1 . \alpha_2 \ldots . \alpha_\lambda . \beta_1 . \beta_2 \ldots . \beta_\mu = 1.2.3 \ldots . \frac{p-1}{2}.$$

Mais d'après la définition même des α et des β, on a

$$\alpha_1 . \alpha_2 \ldots \alpha_\lambda (-\beta_1)(-\beta_2) \ldots (-\beta_\mu) \equiv \mathrm{D}.2\mathrm{D}.3\mathrm{D} \ldots \frac{p-1}{2}\mathrm{D} \pmod{p},$$

c'est-à-dire

$$(-1)^\mu . \alpha_1 . \alpha_2 \ldots \alpha_\lambda . \beta_1 . \beta_2 \ldots \beta_\mu \equiv 1.2 \ldots \frac{p-1}{2} . \mathrm{D}^{\frac{p-1}{2}} \pmod{p}.$$

Il en résulte

$$\mathrm{D}^{\frac{p-1}{2}} \equiv (-1)^\mu \pmod{p}$$

et par suite

$$\left(\frac{\mathrm{D}}{p}\right) = (-1)^\mu$$

On peut remarquer que μ désigne le nombre des restes minima positifs des nombres

$$\mathrm{D}, \ 2\mathrm{D}, \ 3\mathrm{D}, \ \ldots\ldots, \ \frac{p-1}{2}\mathrm{D}$$

qui sont plus grands que $\frac{p}{2}$.

L'application au cas où $\mathrm{D} = 2$ est immédiate ; les restes minima de ces nombres sont ces nombres eux-mêmes :

$$2, \ 4, \ 6, \ \ldots\ldots, \ p-1,$$

et μ est égal au nombre des nombres pairs compris entre $\frac{p}{2}$ et p, ou, ce qui revient au même, au nombre des nombres entiers compris

entre $\frac{p}{4}$ et $\frac{p}{2}$. Si $\frac{p-1}{2}$ est pair, ce nombre est égal à $\frac{p-1}{4}$; si $\frac{p-1}{2}$ est impair, ce nombre est égal à $\frac{p+1}{4}$; dans le premier cas $\frac{p+1}{2}$ est impair et l'on peut écrire

$$\mu \equiv \frac{p+1}{2}\mu \pmod{2}.$$

Or $$\frac{p+1}{2}\mu = \frac{p+1}{2}\cdot\frac{p-1}{4} = \frac{p^2-1}{8}.$$

Dans le second cas, on a de même

$$\mu \equiv \frac{p-1}{2}\mu \equiv \frac{p^2-1}{8} \pmod{2}.$$

Donc dans tous les cas, on a

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}},$$

ce qui donne les règles énoncées plus haut.

42. Si nous revenons au cas général, nous voyons que le nombre désigné par μ est défini lorsque p est un nombre impair, qui n'est pas nécessairement premier. On peut convenir de représenter par $\left(\frac{D}{p}\right)$ la valeur de $(-1)^{\mu}$, dans le cas où p n'est pas premier ; mais *le symbole ainsi défini n'a de signification quadratique que lorsque p est un nombre premier* ; il coïncide dans ce cas avec le symbole de Legendre. M. Schering et Kronecker ont montré que le symbole ainsi généralisé a les propriétés du symbole de Legendre. On peut remarquer d'abord que dans le calcul relatif au nombre 2, on n'a jamais supposé que p soit premier ; on a donc toujours

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}},$$

p étant un nombre impair quelconque. De même si $D = -1$, on voit immédiatement que tous les restes minima absolus sont négatifs ; on a donc

$$\mu = \frac{p-1}{2}$$

et par suite, d'après la définition même du symbole généralisé,

$$\left(\frac{-1}{p}\right) = (-1)^{\mu} = (-1)^{\frac{p-1}{2}}.$$

Pour généraliser les autres propriétés élémentaires du symbole de Legendre, il est commode de se servir d'une expression analytique de $(-1)^{\mu}$, expression qui d'ailleurs nous sera utile dans la suite.

Nous représenterons par $\mathfrak{R}(x)$ le reste minimum absolu du nombre x par rapport à p, de sorte que $\frac{\mathfrak{R}(x)}{p}$ est inférieur à $\frac{1}{2}$ en valeur absolue et que l'on a

$$\mathfrak{R}(x) \equiv x \pmod{p}.$$

Si en adoptant une notation due à Kronecker, nous désignons. d'une manière générale par sgn. a (prononcez : *signe de* a) l'unité précédée du signe $+$ ou du signe $-$ suivant que a est positif ou négatif, on a

$$\left(\frac{D}{p}\right) = \text{sgn.} \prod_{a=1}^{a=\frac{p-1}{2}} \mathfrak{R}(aD).$$

Cette égalité a été démontrée lorsque p est un nombre premier impair et sert de définition au symbole $\left(\frac{D}{p}\right)$ lorsque p est impair et non premier.

Il est clair que l'on a

$$\mathfrak{R}(x) = \mathfrak{R}(x')$$

si

$$x \equiv x' \pmod{p};$$

et

$$\mathfrak{R}(x) = -\mathfrak{R}(x')$$

si

$$x \equiv -x' \pmod{p}.$$

Il en résulte que la congruence

$$D \equiv D' \pmod{p}$$

entraîne

$$\left(\frac{D}{p}\right) = \left(\frac{D'}{p}\right),$$

ce qui était évident lorsqu'on supposait p premier.

Il nous reste à démontrer l'égalité fondamentale

$$\left(\frac{D}{p}\right)\left(\frac{D'}{p}\right) = \left(\frac{DD'}{p}\right).$$

Soient

$$\alpha_1, \alpha_2, \ldots, \alpha_\lambda; -\beta_1, -\beta_2, \ldots, -\beta_\mu$$

les restes minima absolus des nombres

$$D, 2D, 3D, \ldots, \frac{p-1}{2}D.$$

Les nombres

$$\alpha_1, \alpha_2, \ldots \alpha_\lambda; \beta_1, \beta_2, \ldots \beta_\mu$$

sont égaux, abstraction faite de l'ordre, aux nombres

$$1, 2, 3, \ldots, \frac{p-1}{2}.$$

On peut donc, pour calculer $\left(\frac{D'}{p}\right)$, prendre les restes minima absolus des nombres

$$\alpha_1 D', \alpha_2 D', \ldots \alpha_\lambda D'; \beta_1 D', \ldots, \beta_\mu D'.$$

On peut donc écrire

$$\left(\frac{D'}{p}\right) = \text{sgn.} \prod \mathfrak{R}(\alpha D').\mathfrak{R}(\beta D').$$

Mais on a

$$\mathfrak{R}(\beta D') = -\mathfrak{R}(-\beta D')$$

et le nombre des β est égal à μ : on a donc

$$\left(\frac{D'}{p}\right) = \text{sgn.} (-1)^\mu \prod \mathfrak{R}(\alpha D')\mathfrak{R}(-\beta D')$$

ou bien, en multipliant par $\left(\frac{D}{p}\right)$ ou $(-1)^\mu$,

$$\left(\frac{D}{p}\right)\left(\frac{D'}{p}\right) = \text{sgn.} \prod \mathfrak{R}(\alpha D')\mathfrak{R}(-\beta D').$$

Mais les α et les $-\beta$ sont respectivement congrus aux nombres $D, 2D, \ldots, \frac{p-1}{2}D$; on a donc

$$\left(\frac{D}{p}\right)\left(\frac{D'}{p}\right) = \text{sgn.} \prod_{a=1}^{a=\frac{p-1}{2}} \mathfrak{R}(aD.D') = \left(\frac{DD'}{p}\right).$$

C. Q. F. D.

Donc *pour déterminer le signe du symbole* $\left(\frac{D}{p}\right)$, *on peut décom-*

poser D *en facteurs premiers et considérer les facteurs premiers qui figurent dans* D *avec un exposant impair ; il suffira de faire le produit des symboles relatifs à chacun de ces facteurs.*

Indiquons enfin la représentation analytique du symbole $\left(\frac{D}{p}\right)$ due à *Eisenstein*; elle n'introduit pas de symboles à définition arithmétique, tels que $\mathfrak{R}(x)$ ou sgn. a. Remarquons d'abord que l'on a

$$\text{sgn. }\sin\frac{2\pi a D}{p} = \text{sgn. }\mathfrak{R}(aD)$$

et par suite

$$\left(\frac{D}{p}\right) = \text{sgn.}\prod_{a=1}^{a=\frac{p-1}{2}}\sin\frac{2\pi a D}{p}.$$

Or, a étant inférieur à $\frac{p-1}{2}$, l'on a

$$\text{sgn. }\sin\frac{2\pi a}{p} = +1;$$

donc

$$\left(\frac{D}{p}\right) = \text{sgn.}\prod_{a=1}^{a=\frac{p-1}{2}}\frac{\sin\frac{2\pi a D}{p}}{\sin\frac{2\pi a}{p}}.$$

Mais en valeur absolue, le produit des $\frac{p-1}{2}$ sinus du numérateur a la même valeur que le produit des $\frac{p-1}{2}$ sinus du dénominateur ; on peut donc supprimer le symbole sgn. et écrire

$$\left(\frac{D}{p}\right) = \prod_{a=1}^{a=\frac{p-1}{2}}\frac{\sin\frac{2\pi a D}{p}}{\sin\frac{2\pi a}{p}}.$$

Dans le cas où D est un nombre impair, on voit facilement que l'on peut écrire aussi

$$\left(\frac{D}{p}\right) = \prod_{a=1}^{a=\frac{p-1}{2}}\frac{\sin\frac{\pi a D}{p}}{\sin\frac{\pi a}{p}}.$$

Cette expression analytique a conduit Eisenstein à poser $\left(\frac{D}{p}\right) = 0$, lorsque D n'est pas premier avec p.

IV. — Loi de réciprocité. — Applications.

43. Nous allons démontrer maintenant sur le symbole $\left(\frac{D}{p}\right)$ généralisé une proposition qui se réduit à la loi de réciprocité de Legendre lorsque D et p sont deux nombres premiers. Cette proposition consiste dans l'égalité

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}},$$

dans laquelle p et q sont deux nombres *impairs positifs* quelconques. *Si l'on suppose que* p *et* q *sont premiers*, chacun des symboles qui figurent dans le premier membre a une signification quadratique et la formule se traduit ainsi en langage ordinaire :

Si l'un quelconque des nombres p *et* q *est de la forme* $4n+1$: *si* p *est reste de* q, q *est reste de* p *et si* p *est non-reste de* q, q *est non-reste de* p.

Si, au contraire, p *et* q *sont tous deux de la forme* $4n+3$: *si* p *est reste de* q, q *est non-reste de* p *et si* p *est non-reste de* q, q *est non-reste de* p.

C'est la loi de Legendre.

Nous allons démontrer la proposition plus générale qui vient d'être énoncée. Pour cela écrivons

$$\left(\frac{q}{p}\right) = \text{sgn.} \prod_{a=1}^{a=\frac{p-1}{2}} \mathfrak{R}(aq).$$

Pour que $\mathfrak{R}(aq)$ soit négatif, *il faut et il suffit* qu'il y ait un entier x_1 tel que l'on ait simultanément

$$px_1 > aq,$$

$$px_1 < aq + \frac{p}{2},$$

ou simplement $(aq - px_1)\left(aq - px_1 + \frac{p}{2}\right) < 0.$

D'ailleurs si z désigne un entier différent de x_1 on a

$$(aq - pz)\left(aq - pz + \frac{p}{2}\right) > 0,$$

car, si z est plus petit que x, les deux facteurs sont positifs; si z est plus grand que x, les deux facteurs sont négatifs. Si donc n désigne un entier supérieur ou égal à x_1, on a

$$\text{sgn.}\ \mathfrak{R}(aq) = \text{sgn.}\prod_{x=1}^{x=n}(aq - px)\left(aq - px + \frac{p}{2}\right).$$

Or on a

$$px < aq + \frac{p}{2}$$

et

$$a \leqslant \frac{p-1}{2}.$$

Donc

$$px < \frac{p-1}{2}q + \frac{p}{2} < \frac{p}{2}q + \frac{p}{2},$$

et par suite

$$x < \frac{q+1}{2}$$

ou, puisque q est impair et x entier,

$$x \leqslant \frac{q-1}{2}.$$

On peut donc prendre

$$n = \frac{q-1}{2}$$

et écrire

$$\text{sgn.}\ \mathfrak{R}(aq) = \text{sgn.}\prod_{x=1}^{x=\frac{q-1}{2}}(aq - px)\left(aq - px + \frac{p}{2}\right)$$

Par suite

$$\left(\frac{q}{p}\right) = \text{sgn.}\prod_{a=1}^{a=\frac{p-1}{2}}\mathfrak{R}(aq) = \text{sgn.}\prod_{a=1}^{a=\frac{p-1}{2}}\prod_{x=1}^{x=\frac{q-1}{2}}(aq - px)\left(aq - px + \frac{p}{2}\right)$$

Nous pouvons écrire

$$\left(\frac{q}{p}\right) = \text{sgn.}\prod_{a=1}^{a=\frac{p-1}{2}}\prod_{x=1}^{x=\frac{q-1}{2}}(aq - px) \times \text{sgn.}\prod_{a=1}^{a=\frac{p-1}{2}}\prod_{x=1}^{x=\frac{q-1}{2}}\left(aq - px + \frac{p}{2}\right).$$

Remplaçons dans le dernier produit la variable x par $\frac{q+1}{2} - y$; y variera comme x de 1 à $\frac{q-1}{2}$, et l'on aura

$$aq - px + \frac{p}{2} = aq + py - \frac{pq}{2},$$

d'où

$$\left(\frac{q}{p}\right) = \text{sgn.} \prod_{a=1}^{a=\frac{p-1}{2}} \prod_{x=1}^{x=\frac{q-1}{2}} (aq - px) \times \prod_{a=1}^{a=\frac{p-1}{2}} \prod_{y=1}^{y=\frac{q-1}{2}} \left(aq + py - \frac{pq}{2}\right),$$

ou, en réunissant de nouveau les deux produits et remplaçant x et y par b,

$$\left(\frac{q}{p}\right) = \text{sgn.} \prod_{a=1}^{a=\frac{p-1}{2}} \prod_{b=1}^{b=\frac{q-1}{2}} (aq - bp)\left(aq + bp - \frac{pq}{2}\right).$$

On trouve de même

$$\left(\frac{p}{q}\right) = \text{sgn.} \prod_{a=1}^{a=\frac{p-1}{2}} \prod_{b=1}^{b=\frac{q-1}{2}} (bp - aq)\left(bp + aq - \frac{pq}{2}\right).$$

Donc

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \text{sgn.} \prod_{a=1}^{a=\frac{p-1}{2}} \prod_{b=1}^{b=\frac{q-1}{2}} [-(aq - bp)^2].$$

Le nombre des facteurs est égal à $\frac{p-1}{2} \cdot \frac{q-1}{2}$ puisque a doit prendre $\frac{p-1}{2}$ valeurs et b, $\frac{q-1}{2}$. On a ainsi finalement

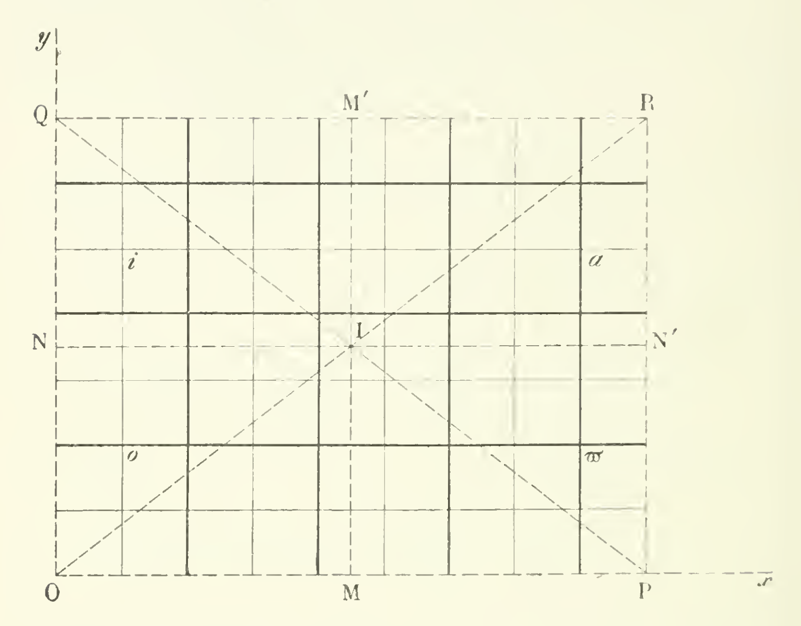
$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

Cette démonstration est due à Kronecker.

44. On peut rendre la démonstration de cette égalité intuitive en s'aidant de quelques considérations géométriques (*).

(*) Cf. *Cayley. Collected Mathematical Papers*, tome II.

Désignons par p et q deux nombres impairs premiers entre eux : traçons deux axes rectangulaires Ox, Oy ; prenons sur Ox une longueur OP égale à p et sur Oy une longueur OQ égale à q.



Achevons le rectangle OPRQ et traçons ses diagonales OR et PQ qui se coupent en I, et ses axes de symétrie $MM'\left(x = \frac{p}{2}\right)$ et $NN'\left(y = \frac{q}{2}\right)$. Nous considérerons uniquement les points de *coordonnées entières* situés *à l'intérieur* de ce rectangle (non sur le périmètre) ; p et q étant impairs et premiers entre eux, aucun de ces points ne se trouve sur les droites MM', NN', OR, PQ. On a tracé sur la figure (faite dans l'hypothèse $p = 9$, $q = 7$) les parallèles aux axes qui déterminent ces points, en forçant le trait pour celles de ces droites dont l'abscisse ou l'ordonnée est paire. Nous désignerons par ϖ ceux de ces points dont les deux coordonnées sont paires, par a ceux dont l'abscisse seule est paire, par o ceux dont l'ordonnée seule est paire et par i ceux dont les deux coordonnées sont impaires.

On aperçoit immédiatement la vérité de propositions telles que la suivante : le symétrique d'un point i par rapport à MM' est un

point a; donc le nombre des points i compris à l'intérieur d'un contour fermé quelconque C est égal au nombre des points a compris à l'intérieur du symétrique C′ de C par rapport à MM′. Nous nous appuierons sur cette proposition ou d'autres analogues pour avoir une expression simple du symbole $\left(\frac{q}{p}\right)$; nous avons vu que l'on a

$$\left(\frac{q}{p}\right) = (-1)^{\mu},$$

μ désignant le nombre des restes minima des nombres

$$q,\ 2q,\ 3q,\ \ldots,\ \frac{p-1}{2}q$$

qui sont supérieurs à $\frac{p}{2}$. Or le reste minimum d'un nombre αq est inférieur ou supérieur à $\frac{p}{2}$ suivant que la partie entière de $\frac{2\alpha q}{p}$ est paire ou impaire. Donc μ est congru, suivant le module 2, à la somme des parties entières des nombres

$$\frac{2q}{p},\ \frac{4q}{p},\ \frac{6q}{p},\ \ldots\ldots,\ \frac{(p-1)q}{p}.$$

Mais la partie entière du nombre $\frac{4q}{p}$ par exemple est égale au nombre des points d'ordonnée entière situés sur la droite

$$x = 4$$

entre l'axe des x et la droite OR dont l'équation est

$$y = \frac{q}{p}x.$$

Donc μ est congru (mod. 2) au nombre des points d'*abscisse paire* et d'*ordonnée entière*, c'est-à-dire des points ϖ et a, *compris à l'intérieur du triangle* OPR. Mais le nombre des points a compris à l'intérieur de OPR est égal au nombre des points ϖ compris à l'intérieur de PRQ ; donc μ est congru (mod. 2) au nombre des points ϖ compris à l'intérieur des triangles OPR et PRQ. Or ces deux triangles ont une partie commune IPR, et les points ϖ compris à l'intérieur de cette partie commune étant comptés deux fois, nous pouvons les supprimer et conclure que μ est congru (mod. 2) au nombre des points ϖ compris à l'intérieur des deux triangles OPI, QRI. On verrait de même que l'on a

$$\left(\frac{p}{q}\right) = (-1)^{\mu'},$$

μ' étant congru (mod. 2) au nombre des points ϖ compris à l'intérieur des deux triangles OQI, PRI ; donc

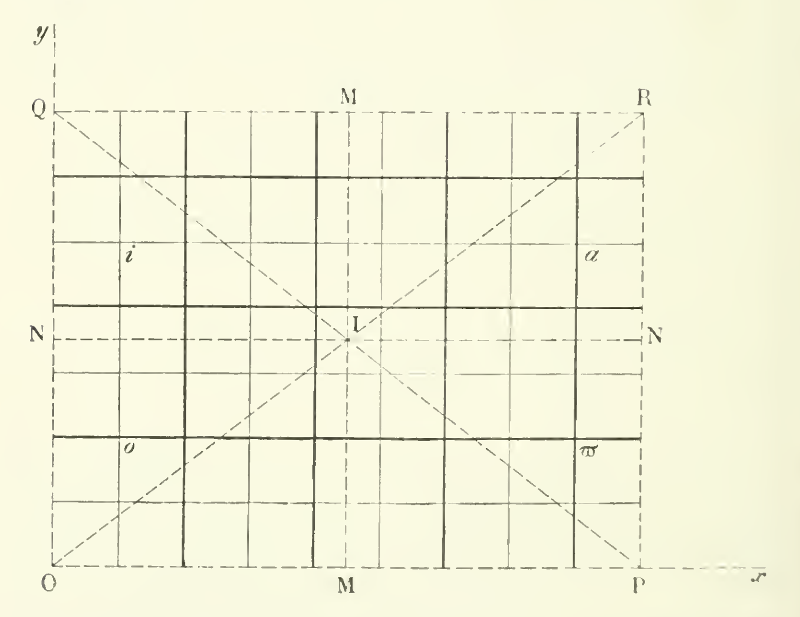
$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\mu+\mu'},$$

$\mu + \mu'$ étant congru (mod. 2) au nombre total des points ϖ situés à l'intérieur du rectangle OPRQ, c'est-à-dire à

$$\frac{p-1}{2} \cdot \frac{q-1}{2},$$

ce que l'on voulait établir.

Cette représentation géométrique permet de démontrer une proposition utilisée comme *lemme* dans certaines démonstrations de la loi de réciprocité.



Le nombre des points ϖ compris à l'intérieur des triangles IMP, IM'R, IM'Q, est égal au nombre des points o, i et a situés à l'intérieur de OMI ; donc le nombre des points ϖ situés à l'intérieur de OPI et RIQ est égal au nombre des points ϖ, a, o et i, c'est-à-dire de tous les points de coordonnées entières situés à l'intérieur de OMI. Or en faisant une transformation homothétique avec un rapport d'homothétie égal à 2, le pôle étant le point O, on voit que le nombre des

points de coordonnées entières situés à l'intérieur de OMI est égal au nombre des points de coordonnées *paires* situés à l'intérieur de OPR (*). Donc μ est congru à ce nombre ; c'est-à-dire que μ *est congru à la somme des parties entières des nombres*

$$\frac{q}{p}, \frac{2q}{p}, \frac{3q}{p}, \ldots\ldots, \frac{\frac{p-1}{2}q}{p}.$$

C'est le lemme dont il vient d'être question. Réciproquement, si on admet ce lemme, la démonstration de la loi de réciprocité est immédiate avec notre figure ; μ est congru au nombre des points ϖ situés à l'intérieur de OPR ; μ' est congru au nombre des points ϖ situés à l'intérieur de OQR ; donc $\mu+\mu'$ est congru au nombre total de ces points, c'est-à-dire à $\frac{p-1}{2}\cdot\frac{q-1}{2}$.

45. Nous pouvons maintenant résoudre d'une manière générale la question que nous nous étions posée : D étant un nombre impair *donné*, trouver un critérium aussi simple que possible faisant connaître le signe de $\left(\frac{D}{p}\right)$. Nous supposons simplement p impair et premier avec D ; si p est un nombre premier, le symbole a une signification quadratique.

On aperçoit immédiatement que l'on a

$$\left(\frac{D}{p}\right) = \left(\frac{p}{D}\right)(-1)^{\frac{p-1}{2}\cdot\frac{D-1}{2}}.$$

Or la valeur de $\left(\frac{p}{D}\right)$ ne dépend que du résidu minimum de p (mod. D) ; la valeur de $(-1)^{\frac{p-1}{2}\cdot\frac{D-1}{2}}$ ne dépend que du résidu minimum de p (mod. 4) (et même en est indépendante si D est de la forme $4n+1$). On en conclut que, dans tous les cas, la valeur de $\left(\frac{D}{p}\right)$ ne dépend que du résidu minimum de p (mod. 4D), résultat que nous avions déjà énoncé sans démonstration ; on voit même que si D est de la forme $4n+1$, il suffit de considérer le résidu minimum de p (mod. 2 D) (**).

(*) Remarquons, en passant que la série de transformations faites a pour résultat de montrer que le nombre des points a situés à l'intérieur de OPR est pair.

(**) On ne considère pas le résidu minimum (mod. D) parce que celui-ci ne serait pas nécessairement impair, et la loi de réciprocité ne s'applique qu'aux nombres impairs.

Soit, par exemple, $D = 3$, on a $4D = 12$; les nombres impairs inférieurs à 12 et premiers avec 3 sont 1, 5, 7, 11 ; on trouve facilement

$$\left(\frac{3}{1}\right) = +1, \qquad \left(\frac{3}{5}\right) = -1, \qquad \left(\frac{3}{7}\right) = -1, \qquad \left(\frac{3}{11}\right) = +1$$

Donc : 3 est résidu quadratique des nombres premiers de l'une des formes $12n + 1$ et $12n + 11$ et non-résidu des nombres premiers de l'une des formes $12n + 5$ et $12n + 7$.

Prenons comme second exemple $D = 5$; D étant ici de la forme $4n + 1$, il suffit de considérer les nombres impairs premiers avec D et inférieurs à $2D$; ce sont 1, 3, 7, 9 : on trouve

$$\left(\frac{5}{1}\right) = +1, \qquad \left(\frac{5}{3}\right) = -1, \qquad \left(\frac{5}{7}\right) = -1, \qquad \left(\frac{5}{9}\right) = +1.$$

Donc : 5 est résidu quadratique des nombres premiers de l'une des formes $10n + 1$ et $10n + 9$ et non-résidu des nombres premiers de l'une des formes $10n + 3$ et $10n + 7$.

46. La loi de réciprocité permet aussi de déterminer facilement la valeur du symbole $\left(\frac{D}{p}\right)$ lorsque D et p sont de grands nombres. Nous allons nous contenter d'indiquer le principe de la méthode employée, sans entrer dans des détails sur les simplifications que l'on peut y apporter.

Supposons par exemple $D < p$; sinon on remplacerait D par son résidu minimum (mod. p). La loi de réciprocité donne

$$\left(\frac{D}{p}\right) = \left(\frac{p}{D}\right)(-1)^{\frac{p-1}{2}\cdot\frac{D-1}{2}};$$

mais si nous désignons par p' le résidu minimum de p (mod. D), on a

$$\left(\frac{p}{D}\right) = \left(\frac{p'}{D}\right).$$

On est donc ramené à calculer un symbole analogue, mais dans lequel les deux termes sont respectivement inférieurs à ceux du symbole proposé ; on pourra continuer de même, jusqu'à ce qu'on arrive à des nombres très simples.

Il faut remarquer que la loi de réciprocité ne s'applique qu'aux

nombres impairs ; par suite, si p' par exemple est pair, on devra le décomposer en un produit d'un facteur impair et d'une puissance de 2. Si l'exposant de cette puissance est impair, on devra appliquer la règle qui donne le caractère quadratique du nombre 2. On peut aussi éviter d'avoir à écrire des nombres pairs, en prenant tantôt le résidu minimum positif, tantôt le résidu minimum négatif; pour un module impair, l'un des deux est toujours impair. Mais on devra se servir du caractère quadratique de -1, ou bien de la loi de réciprocité généralisée pour les nombres négatifs; si l'on pose *par définition*

$$\left(\frac{D}{-p}\right) = -\left(\frac{D}{p}\right),$$

p étant positif et D positif ou négatif, on constate que la loi de réciprocité s'exprime par la formule

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}+(\varepsilon-1)(\eta-1)},$$

ε et η étant respectivement égaux à 1 ou à zéro suivant que p et q sont positifs ou négatifs ; en d'autres termes la loi de réciprocité subsiste, à moins que les deux nombres p et q ne soient négatifs.

En combinant les remarques précédentes, on arrive très simplement au résultat.

Soit par exemple à trouver la valeur de $\left(\frac{436}{875}\right)$.

On a $436 = 2^2.109$; donc

$$\left(\frac{436}{875}\right) = \left(\frac{109}{875}\right).$$

D'ailleurs $109 = 4.27 + 1$; donc

$$\left(\frac{109}{875}\right) = \left(\frac{875}{109}\right) = \left(\frac{8.109+3}{109}\right) = \left(\frac{3}{109}\right),$$

et puisque 109 est de la forme $4n+1$:

$$\left(\frac{3}{109}\right) = \left(\frac{109}{3}\right) = \left(\frac{1}{3}\right) = +1.$$

Donc

$$\left(\frac{436}{875}\right) = +1.$$

Il faut remarquer que, 875 n'étant pas premier, ce symbole n'a pas de signification quadratique ; on aurait donc pu procéder autrement, en décomposant en leurs facteurs premiers le numérateur et le dénominateur. On a de cette manière

$$\left(\frac{436}{875}\right) = \left(\frac{2^2 . 109}{5^3 . 7}\right) = \left(\frac{109}{5}\right) \cdot \left(\frac{109}{7}\right) = \left(\frac{4}{5}\right) \cdot \left(\frac{4}{7}\right) = +1.$$

CHAPITRE V

DÉCOMPOSITION DES NOMBRES EN CARRÉS. — APPLICATIONS

I. — Formes en général. — Sommes de carrés.

47. Un des problèmes les plus importants de la théorie des nombres est celui de la *représentation des nombres par les formes*. Nous ne pouvons pas songer ici à parler de tous les travaux auxquels ce problème a donné lieu; nous allons simplement en étudier quelques cas simples, choisis de manière à constituer une application immédiate des théories précédentes et à conduire à des notions nouvelles intéressantes.

On sait que l'on désigne en Algèbre sous le nom de *forme* tout polynome homogène; on distingue dans une forme deux choses essentielles : le degré de la forme et le nombre des variables. Les formes des degrés 1, 2, 3, 4 sont dites *linéaires*, *quadratiques*, *cubiques*, *biquadratiques*; les formes à deux, trois, quatre variables sont dites *binaires, ternaires, quaternaires*. Ainsi

$$ax^3 + byzt$$

est une forme *cubique quaternaire* ; a et b sont les coefficients de la forme ; x, y, z, t les variables. Une forme à coefficients *réels* est dite *définie* lorsqu'elle garde toujours le même signe, quelles que soient les valeurs *réelles* attribuées aux variables ; une forme peut être *définie positive* (par exemple $x^2 + y^2$) ou *définie négative* (par exemple : $-x^4 - y^4 - z^4$); une forme *non définie* est dite *indéfinie*. Une forme indéfinie peut pour des valeurs réelles des variables prendre une valeur réelle *quelconque* donnée à l'avance ;

une forme définie peut prendre *toutes* les valeurs d'un certain signe et celles-là seulement.

Nous avons rappelé ces définitions parce qu'elles subsistent en Arithmétique ; seulement, on suppose essentiellement que les coefficients des formes sont des *nombres entiers* (positifs ou négatifs) et que les variables prennent seulement des *valeurs entières*. Dès lors, la valeur numérique de la forme est toujours un nombre entier ; de plus, il est facile de s'assurer, qu'en général, cela ne peut pas être un nombre entier quelconque ; par exemple, la forme $x^2 + 2y^2$ ne prend jamais la valeur 5 quelles que soient les valeurs *entières* de x et de y. Le problème de la *représentation des nombres par les formes* est dès lors le suivant : *étant donnée une forme, trouver les nombres entiers auxquels elle peut devenir égale* (pour des valeurs entières des variables, bien entendu) : on dit que ces nombres peuvent être *représentés* par la forme.

Avant d'étudier des cas particuliers de ce problème, nous allons présenter quelques remarques sur le cas général.

48. On se propose de rechercher quels sont les nombres susceptibles d'être représentés par la forme de degré n

$$\varphi(x, y, z).$$

Soit A_0 l'un de ces nombres :

$$A_0 = \varphi(x_0, y_0, z_0).$$

On aura, k désignant un entier quelconque,

$$k^n A_0 = \varphi(kx_0, ky_0, kz_0),$$

c'est-à-dire que de la représentation du nombre A_0, on déduit une représentation du nombre $k^n A_0$. Cette dernière représentation est dite *impropre* ; on donne inversement le nom de représentation *propre* à toute représentation dans laquelle les valeurs des variables sont des nombres *premiers entre eux dans leur ensemble*. Il est clair qu'une représentation propre ne peut être déduite d'une autre par le procédé employé tout à l'heure ; au contraire, toute représentation impropre peut être déduite de cette manière d'une représentation propre et d'une seule. On en conclut qu'il suffit d'étudier les représentations propres. Par exemple pour trouver toutes les représentations possibles du nombre $p^{2n}q^n A_0$ (p et q étant des nombres premiers et A_0 n'étant divisible par la puissance $n^{ième}$ d'aucun nombre

premier) par la forme de degré n : $\varphi(x, y, z)$, il suffira de chercher les représentations *propres* des nombres

$$p^{2n}q^nA_0, \quad p^nq^nA_0, \quad q^nA_0, \quad p^{2n}A_0, \quad p^nA_0, \quad A_0.$$

On a ainsi décomposé le problème en plusieurs autres qui sont essentiellement distincts.

Il est donc naturel d'étudier surtout les représentations propres ; un premier exemple nous convaincra d'ailleurs de l'avantage qu'il peut y avoir à les considérer exclusivement.

Nous allons nous occuper des formes qui sont des sommes de carrés :

$$x^2 + y^2 + z^2 + \ldots\ldots$$

et nous supposerons *essentiellement* que les nombres $x, y, z, \ldots\ldots$ sont *premiers entre eux dans leur ensemble*. Cette hypothèse va nous permettre d'établir des théorèmes intéressants sur les sommes de *deux* et de *quatre* carrés.

49. Le premier de ces théorèmes est en quelque sorte un théorème d'Algèbre; il consiste en ce que *le produit de la somme de deux carrés par la somme de deux carrés est aussi la somme de deux carrés ;* de même *le produit de la somme de quatre carrés par la somme de quatre carrés est aussi la somme de quatre carrés*. Il faut entendre ici par le mot *carré* : carré d'une fonction entière à coefficients entiers d'indéterminées d'ailleurs quelconques.

Il suffit, pour vérifier ces propositions, d'écrire les identités

$$(a^2 + b^2)(\alpha^2 + \beta^2) = (a\alpha + b\beta)^2 + (a\beta - b\alpha)^2$$

et

$$(a^2 + b^2 + c^2 + d^2)(\alpha^2 + \beta^2 + \gamma^2 + \delta^2) = A^2 + B^2 + C^2 + D^2,$$

où l'on a posé :

$$\begin{aligned} A &= a\alpha + b\beta + c\gamma + d\delta, \\ B &= a\beta - b\alpha + c\delta - d\gamma, \\ C &= a\gamma - c\alpha + d\beta - b\delta, \\ D &= a\delta - d\alpha + b\gamma - c\beta. \end{aligned}$$

Si, en particulier, on suppose que $a, b, c, d, \alpha, \beta, \gamma, \delta$ sont des nombres entiers, on a des théorèmes d'arithmétique; c'est de ces théorèmes que nous allons nous occuper actuellement pour en démontrer en quelque sorte la réciproque : si un nombre premier

divise la somme des carrés de deux ou quatre entiers *sans diviser tous ces entiers*, il est lui-même la somme de deux ou de quatre carrés. On voit aisément que cet énoncé revient au suivant : *si un nombre divise la somme de deux ou quatre carrés premiers entre eux* (dans leur ensemble), *il est lui-même la somme de deux ou quatre carrés.*

Nous ne donnerons la démonstration que pour le cas de quatre carrés, en ajoutant que, dans le cas de deux carrés, elle est fondée sur le même principe et est plus simple.

Supposons donc que p divise la somme $a^2 + b^2 + c^2 + d^2$, où a, b, c, d sont premiers entre eux. Nous pouvons remplacer a, b, c, d par leurs résidus minima absolus par rapport à p ; nous désignerons par a', b', c', d' ces résidus inférieurs ou au plus égaux à $\frac{p}{2}$; ils ne peuvent être tous les quatre égaux à $\frac{p}{2}$ puisqu'ils sont premiers entre eux; on a donc

$$a'^2 + b'^2 + c'^2 + d'^2 < 4\left(\frac{p}{2}\right)^2,$$

le signe $<$ excluant l'égalité. (On suppose $p > 2$; $2 = 1^2 + 1^2$ est la somme de deux carrés). Donc on peut poser

$$(1) \qquad a'^2 + b'^2 + c'^2 + d'^2 = pp',$$

p' étant *inférieur* à p ; si p' était égal à 1, on aurait mis p sous la forme de la somme de quatre carrés ; supposons $p' > 1$ et soient

$$a' - \alpha p', \qquad b' - \beta p', \qquad c' - \gamma p', \qquad d' - \delta p'$$

les résidus minima absolus de a', b', c', d' par rapport à p' (ils ne sont pas tous nuls, sinon a, b, c, d ne seraient pas premiers entre eux) ; on a

$$(2) \quad (a' - \alpha p')^2 + (b' - \beta p')^2 + (c' - \gamma p')^2 + (d' - \delta p')^2 = p'p'',$$

p'' étant inférieur à p' et par suite inférieur à p. En multipliant membre à membre les égalités (1) et (2), on obtient

$$A^2 + B^2 + C^2 + D^2 = pp'^2p''$$

avec

$$A = a'^2 + b'^2 + c'^2 + d'^2 - (a'\alpha + b'\beta + c'\gamma + d'\delta)p' = p'(p - a'\alpha - b'\beta - c'\gamma - d'\delta),$$

$$B = (b'\alpha - a'\beta - c'\gamma + d'\delta)p',$$

$$C = (c'\alpha - a'\gamma - d'\beta + b'\delta)p',$$

$$D = (d'\alpha - a'\delta - b'\gamma + c'\beta)p',$$

c'est-à-dire des valeurs de la forme

$$A = a''p', \qquad B = b''p', \qquad C = c''p', \qquad D = d''p'.$$

On en conclut

(3) $$a''^2 + b''^2 + c''^2 + d''^2 = pp'',$$

égalité de la même forme que (1), mais où p'' est inférieur à p' : si p'' n'est pas égal à un, on opérera de même, et on obtiendra une série d'égalités :

$$a'''^2 + b'''^2 + c'''^2 + d'''^2 = pp''',$$

$$\cdots\cdots\cdots\cdots$$

$$\cdots\cdots\cdots\cdots$$

$$a_n^2 + b_n^2 + c_n^2 + d_n^2 = pp_n.$$

p', p'', p''', ... , p_n étant des entiers décroissants et ne pouvant être nuls ; il arrivera nécessairement que l'un d'eux sera égal à l'unité, et l'égalité correspondante prouvera que p est la somme de quatre carrés.

50. Il est maintenant facile de démontrer que *tout entier est la somme de quatre carrés au plus*. Il suffit pour cela de faire voir que tout *nombre premier* est la somme de quatre carrés au plus. Nous allons le montrer pour les nombres premiers de la forme $4n + 3$; nous verrons ensuite que tout nombre premier de la forme $4n + 1$ est la somme de deux carrés. Enfin on a déjà remarqué que 2 est la somme de deux carrés.

Soit p un nombre premier de la forme $4n + 3$; considérons la série des nombres

$$1,\ 2,\ 3,\ \ldots\ldots\ p - 1.$$

Le premier, 1, est résidu quadratique de p ; le dernier, $p - 1$, est non-résidu ; il y a donc certainement dans la suite un résidu α suivi d'un non-résidu $\alpha + 1$; -1 étant non-résidu de p, $-\alpha - 1$ est résidu ; on peut donc trouver des nombres t et u satisfaisant aux congruences

$$t^2 \equiv \alpha \pmod{p},$$

$$u^2 \equiv -\alpha - 1 \pmod{p}.$$

On en conclut

$$t^2 + u^2 + 1 \equiv 0 \pmod{p}.$$

Donc p divise la somme de *trois* carrés premiers entre eux $t^2 + u^2 + 1$; donc p est la somme de quatre carrés au plus.

Il est bon de remarquer que p, nombre premier de la forme

$4n+3$, ne peut pas être la somme de deux carrés ; en effet, si l'on avait

$$p = t^2 + u^2,$$

on en conclurait

$$t^2 \equiv \alpha \pmod{p},$$

$$u^2 \equiv -\alpha \pmod{p},$$

et par suite -1 serait résidu quadratique de p, ce qui est impossible.

Ceci nous montre que les nombres premiers q de la forme $4n+1$ sont la somme de deux carrés, *à l'exclusion de tous les autres;* en effet, -1 est résidu quadratique ; donc la congruence

$$x^2 + 1 \equiv 0 \quad (mod.\ q)$$

a une racine, c'est-à-dire : q divise la somme de deux carrés premiers entre eux.

Cette propriété des nombres premiers q de la forme $4n+1$ est si importante, que nous croyons devoir en donner plusieurs démonstrations, d'ailleurs intéressantes par elles-mêmes.

Elles sont toutes fondées sur ce qu'un nombre divisant la somme de deux carrés est lui-même la somme de deux carrés ; ce qui les distingue, c'est la manière dont on obtient la somme de deux carrés divisible par le nombre premier $4n+1$.

Le théorème de Wilson nous en fournit immédiatement une. Soit en effet $q = 4n+1$ un nombre premier ; on a

$$1.2.3.\ldots\ldots 4n + 1 \equiv 0 \pmod{q}.$$

Mais

$$1 \equiv -4n \pmod{q},$$

$$2 \equiv -(4n-1) \pmod{q},$$

$$\cdots\cdots\cdots$$

$$\cdots\cdots\cdots$$

$$2n \equiv -(2n+1) \pmod{q}.$$

Ces congruences étant en nombre pair, on obtient, en les multipliant membre à membre,

$$1.2.\ldots.2n \equiv (2n+1)(2n+2)\ldots.4n \quad (mod.\ q).$$

Le théorème de Wilson se trouve dès lors exprimé par la congruence

$$[1.2.\ldots.(2n-1)2n]^2 + 1 \equiv 0 \quad (mod.\ q),$$

qui exprime bien que q divise la somme de deux carrés.

51. Une autre démonstration, due à M. Smith, fait appel à des considérations toutes différentes.

Considérons une fraction continue limitée, dans laquelle les quotients incomplets sont des entiers positifs :

$$a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}}$$

On sait qu'elle est égale à une fraction toujours irréductible, qui s'écrit

$$\frac{(a_1, a_2, \ldots, a_n)}{(a_2, a_3, \ldots, a_n)},$$

en représentant, d'une manière générale, par

$$(a_1, a_2, \ldots, a_k)$$

une fonction facile à calculer des lettres $a_1, a_2, \ldots, a_k$. Nous appellerons, pour un instant, fonctions F, ces fonctions qui sont ainsi numérateurs ou dénominateurs de réduites.

Ces fonctions F ont des propriétés très simples ; nous démontrerons tout à l'heure les deux suivantes :

$$(\alpha) \qquad (a_1, a_2, \ldots, a_n) = (a_n, a_{n-1}, \ldots a_1),$$

$$(\beta) \qquad (a_1, a_2, \ldots, a_p, a_{p+1}, \ldots a_n) = (a_1, a_2 \ldots, a_p)(a_{p+1}, \ldots, a_n) + (a_1, a_2 \ldots, a_{p-1})(a_{p+2}, \ldots a_n).$$

Considérons en particulier des fonctions F pour lesquelles les quotients incomplets équidistants des extrêmes soient égaux :

$$a_k = a_{n-k}.$$

Nous distinguerons le cas où n est pair de celui où n est impair. Soit d'abord $n = 2p$; nous avons, d'après l'égalité (β),

$$(a_1, a_2, \ldots, a_n) = (a_1, \ldots, a_p)(a_p, \ldots, a_1) + (a_1, \ldots, a_{p-1})(a_{p-1}, \ldots, a_1)$$

ou, d'après (α),

$$(a_1, a_2, \ldots, a_n) = (a_1, \ldots, a_p)^2 + (a_1, \ldots, a_{p-1})^2,$$

c'est-à-dire qu'une fonction F de cette forme est une somme de deux carrés. Si n est impair et égal à $2p - 1$, on obtient de même

$$F = (a_1, \ldots, a_n) = (a_1, \ldots, a_{p-1})[(a_1, \ldots, a_p) + (a_1, \ldots, a_{p-2})],$$

c'est-à-dire que dans ce cas F n'est pas un nombre premier (une discussion facile exclut le cas où l'un des facteurs du second membre serait égal à l'unité; cela ne peut arriver si $a_1 > 1$).

Ceci posé, M. Smith a cherché à représenter un nombre quelconque P par une fonction F, dans laquelle a_1 est supérieur à l'unité. Dans une fraction continue limitée, on peut toujours supposer $a_n \neq 1$, ou bien $a_n = 1$ (*); je ferai la première hypothèse. Ceci posé, la fraction continue dans laquelle a_1 et a_n sont supérieurs à 1, ne peut provenir que d'une fraction ordinaire ayant pour numérateur p et pour dénominateur un nombre q inférieur à $\frac{p}{2}$ et premier avec p. Soit

$$\frac{(a_1, a_2, \ldots, a_n)}{(a_2, \ldots, a_n)} = \frac{p}{q}.$$

On aura

$$\frac{(a_n, a_{n-1}, \ldots, a_1)}{(a_{n-1}, \ldots, a_1)} = \frac{p}{q'},$$

et q' sera pour la même raison que q, premier avec p et inférieur à $\frac{p}{2}$. On fait ainsi correspondre à chaque fraction $\frac{p}{q}$ une fraction $\frac{p}{q'}$ présentant les mêmes quotients incomplets dans l'ordre inverse. Il peut se faire que l'on ait $q = q'$; alors, mais seulement alors, les termes équidistants des extrêmes seront égaux; c'est ce qui arrivera nécessairement si le nombre des nombres inférieurs à $\frac{p}{2}$ et premiers avec p (en excluant l'unité qui ne donne rien) est impair: car ces nombres se correspondant deux à deux, il y en aura nécessairement un qui se correspondra à lui-même. Tout nombre p satisfaisant à cette condition peut être représenté par une fonction F dans laquelle les quotients incomplets équidistants des extrêmes

(*) Pour cela, bien entendu, il peut être nécessaire de changer d'une unité la valeur de n.

sont égaux ; il est donc la somme de deux carrés ou le produit de deux facteurs ; nous excluons ce dernier cas en considérant un nombre p *premier*. Pour que le nombre des entiers inférieurs à $\frac{p}{2}$ et premiers avec p (non compris l'unité) soit impair, il faut supposer $p = 4n+1$; nous arrivons donc à cette conclusion que *tout nombre premier de la forme* $4n+1$ *est la somme de deux carrés.*

Il nous reste à établir les deux propriétés des fonctions F sur lesquelles nous nous sommes appuyés. La première (α) résulte immédiatement de la représentation des fonctions F par les déterminants ; on vérifie en effet que

$$(a_1, a_2, \ldots\ldots a_n) = \begin{vmatrix} a_1 & u & 0 & 0 & \ldots & 0 \\ v & a_2 & u & 0 & \ldots & 0 \\ 0 & v & a_3 & u & \ldots & 0 \\ 0 & \ldots & \ldots & \ldots & \ldots & 0 \\ 0 & \ldots & \ldots & v & a_{n-1} & u \\ 0 & \ldots & \ldots & \ldots & v & a_n \end{vmatrix}$$

u et v étant deux nombres assujettis à la seule condition $uv = -1$. Cela est évident pour $n=1$ et $n=2$ et on le démontre de proche en proche en développant le déterminant suivant les éléments de la dernière ligne ou de la dernière colonne et appliquant l'identité bien connue dans la théorie des fractions continues (*) :

$$P_n = a_n P_{n-1} + P_{n-2}.$$

En développant le déterminant d'après la règle de Laplace par rapport aux éléments des p premières lignes, on obtient précisément la relation (β).

On peut d'ailleurs la démontrer sans faire appel à la théorie des déterminants.

Considérons deux indéterminées x_0 et x_1 et déduisons-en les quantités $x_2, x_3, \ldots,\ x_{n+1}$ par les relations

$$\begin{aligned} x_2 &= a_1x_1 + x_0, \\ x_3 &= a_2x_2 + x_1, \\ &\ldots\ldots \\ x_{n+1} &= a_nx_n + x_{n-1}. \end{aligned}$$

(*) On a des formes particulièrement intéressantes en supposant $u = 1$, $v = -1$, ou $u = v = \sqrt{-1}$. On pourrait aussi ne pas supposer tous les u, ni tous les v égaux entre eux pourvu que le produit des *correspondants* fût égal à -1.

Il est clair que l'on a

$$x_{n+1} = (a_1, a_2, \ldots, a_n)x_1 + (a_2, \ldots, a_n)x_0.$$

Mais nous pouvons calculer x_{n+1} en partant de x_p et x_{p+1}, de la même manière qu'en partant de x_0 et de x_1 : on obtient ainsi

$$x_{n+1} = (a_{p+1}, \ldots, a_n)x_{p+1} + (a_{p+2}, \ldots a_n)x_p.$$

Or,

$$x_p = (a_1, \ldots, a_{p-1})x_1 + (a_2, \ldots, a_{p-1})x_0,$$

$$x_{p+1} = (a_1, \ldots, a_p)x_1 + (a_2, \ldots, a_p)x_0.$$

En identifiant les coefficients de x_1 dans les deux expressions de x_{n+1} on obtient la relation cherchée :

$$(a_1, \ldots, a_n) = (a_1, \ldots, a_p)(a_{p+1}, \ldots, a_n) + (a_1, \ldots a_{p-1})(a_{p+2}, \ldots a_n).$$

II. — Nombres complexes de Gauss.

52. Nous allons maintenant indiquer les conséquences importantes de ce fait que les nombres premiers de la forme $4n+1$ sont, à l'exclusion des autres, décomposables en sommes de deux carrés.

Pour cela, il est nécessaire d'introduire la notion de nombres entiers complexes. De même qu'en Algèbre, il y a avantage pour beaucoup de questions d'arithmétique à considérer des nombres complexes de la forme $a+bi$, dans lesquels i désigne un symbole soumis aux règles de calcul ordinaires, avec cette restriction que l'on réduit toujours un polynome en i au reste de sa division par i^2+1. Nous ne rappelons pas ici la théorie algébrique des nombres complexes, sur laquelle nous aurons à revenir dans la seconde partie pour l'exposer d'une façon systématique; il suffit ici de supposer connue l'une quelconque des théories ordinaires : nous tenons seulement à faire remarquer que les nombres ainsi introduits sont essentiellement différents de ceux que nous avons appelés *imaginaires de Galois;* nous pensons qu'il ne peut résulter aucune confusion de l'emploi d'un même symbole i dans ces deux théories. Dans les imaginaires de Galois, ce symbole est défini par la *congruence* irréductible

$$f(i) \equiv 0 \pmod{p};$$

ici, par l'*égalité*

$$i^2 + 1 = 0.$$

Considérons donc une expression de la forme $a+bi$, a et b désignant des entiers positifs ou négatifs. C'est ce que nous appelons un entier complexe ; $a-bi$ sera le nombre conjugué ; leur produit a^2+b^2 s'appellera la *norme* de chacun d'eux. (C'est le carré de ce qu'on appelle ordinairement le module). Un entier sera dit une *unité* lorsque sa norme sera égale à 1 ; il y a donc *quatre* unités : $+1$, -1, $+i$, $-i$.

Nous allons montrer que l'on peut établir pour ces entiers complexes, une théorie de la divisibilité toute pareille à celle qu'on a faite pour les nombres entiers.

Soient $a+bi$ et $c+di$ deux nombres complexes ; on a

$$\frac{a+bi}{c+di}=\frac{ac+bd}{c^2+d^2}+\frac{bc-ad}{c^2+d^2}i.$$

Soient x et y deux entiers quelconques ; on peut écrire

$$\frac{a+bi}{c+di}=x+yi+\left(\frac{ac+bd}{c^2+d^2}-x\right)+i\left(\frac{bc-ad}{c^2+d^2}-y\right)$$

ou enfin

$$a+bi=(c+di)(x+yi)+\left[\frac{ac+bd}{c^2+d^2}-x+i\left(\frac{bc-ad}{c^2+d^2}-y\right)\right](c+di).$$

Cette égalité est tout à fait de même forme que l'égalité fondamentale

$$A=BQ+R,$$

qui sert de base à la théorie de la divisibilité des nombres entiers ; seulement dans cette dernière, on sait que Q est choisi de manière que l'on ait

$$R<B,$$

et c'est sur ce fait de la décroissance successive des restes qu'est basée la théorie du plus grand commun diviseur.

Nous allons chercher à trouver une égalité analogue pour la *norme* du *reste* $r+si$ défini par l'égalité

$$a+bi-(c+di)(x+yi)=r+si.$$

On peut choisir x et y de manière que l'on ait

$$\left|\frac{ac+bd}{c^2+a^2}-x\right|\leqslant\frac{1}{2},\qquad \frac{bc-ad}{c^2+d^2}-y\leqslant\frac{1}{2}.$$

Dès lors la norme de $\dfrac{ac+bd}{c^2+d^2}-x+i\left(\dfrac{bc-ad}{c^2+d^2}-y\right)$ est au plus

égale à $\left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2}$, et comme la norme d'un produit est égale au produit des normes des facteurs, on en conclut que la norme de

$$r + si = \left[\frac{ac + bd}{c^2 + d^2} - x + i\left(\frac{bc - ad}{c^2 + d^2} - y\right)\right](c + di)$$

est au plus égale à $\frac{1}{2}(c^2 + d^2)$.

Il est inutile d'aller plus loin ; nous sommes assurés qu'on pourra transporter ici sans modification l'algorithme du plus grand commun diviseur et toutes les conséquences qui s'y rattachent, en particulier la théorie des nombres premiers, définis comme n'admettant pas d'autres diviseurs que *les unités* et leur quotient par les diverses unités ; par exemple $a + bi$ est divisible par : $a + bi$, $-a - bi$, $b - ai$, $-b + ai$. Ces quatre nombres sont dits *associés*. Si l'on considère deux nombres associés comme équivalents, on démontre que tout nombre ne peut être décomposé en facteurs premiers que d'une seule manière.

53. Nous pouvons maintenant démontrer le théorème fondamental, qui nous permettra de trouver immédiatement les nombres premiers complexes :

Pour qu'un entier complexe soit premier, il faut et il suffit que sa norme soit un nombre premier réel.

La condition est suffisante ; car si l'on a

$$a + bi = (r + si)(u + vi),$$

on en conclut

$$a^2 + b^2 = (r^2 + s^2)(u^2 + v^2) ;$$

donc $a + bi$ ne peut être premier que si $a^2 + b^2$ l'est. Il est à peine utile de remarquer que l'on suppose $r^2 + s^2$ et $u^2 + v^2$ différents de l'unité ; sinon $r + si$ et $u + vi$ seraient des unités complexes.

Réciproquement, si $a + bi$ est premier, $a - bi$ l'est aussi : je dis qu'il en résulte que $a^2 + b^2$ est un nombre premier, au sens ordinaire du mot. En effet, si $a^2 + b^2$ avait un diviseur, celui-ci serait décomposable en une somme de deux carrés ; on aurait donc

$$\begin{aligned}(a + bi)(a - bi) = (a^2 + b^2) &= (r^2 + s^2)(u^2 + v^2) \\ &= (r + si)(r - si)(u + vi)(u - vi).\end{aligned}$$

Or l'égalité qu'on obtient en rapprochant les deux membres extrêmes est impossible, puisque le premier membre est le produit de *deux* facteurs premiers complexes, le second d'au moins *quatre*, et qu'un nombre ne peut être décomposé en facteurs premiers que d'une seule manière.

On conclut de ce qui précède que, pour avoir tous les nombres premiers complexes, il suffit de prendre les nombres premiers réels qui sont la somme de deux carrés et de les décomposer en un produit de deux facteurs. Or ces nombres premiers réels sont :

1° Le nombre 2 ;

2° Les nombres premiers impairs de la forme $4n+1$.

Donc, dans le domaine des entiers complexes, on distinguera trois sortes de nombres premiers :

1° Le nombre $1+i$, diviseur de 2 (et son associé $1-i$);

2° Les nombres $a+bi$ tels que l'on ait $a^2+b^2=p$, p étant un nombre premier réel de la forme $4n+1$;

3° Les nombres premiers réels de la forme $4n+3$.

Nous pouvons d'ailleurs remarquer qu'un nombre premier réel de la forme $4n+1$ ne peut être décomposé que d'une manière en la somme de deux carrés.

On ne peut avoir, en effet,

$$p=(a+bi)(a-bi)=(c+di)(c-di),$$

car d'après ce qui précède, ces facteurs imaginaires sont premiers, et le nombre p ne peut être décomposé en facteurs premiers que d'une seule manière.

On voit la distinction capitale établie par ces considérations entre les nombres premiers de la forme $4n+1$ et ceux qui sont de la forme $4n+3$. Ces derniers seuls doivent maintenant être considérés comme de véritables nombres premiers.

Cette distinction n'est pas purement spéculative ; nous avons déjà vu, à propos de la loi de réciprocité des restes quadratiques, que ces deux classes de nombres premiers ont des propriétés tout à fait différentes ; c'est ce qu'on aperçoit davantage encore lorsqu'on étudie les restes biquadratiques, par exemple.

Pour ces derniers, on ne peut donner une généralisation simple de la loi de réciprocité qu'en introduisant les nombres complexes ;

c'est même à cette occasion que Gauss a été amené pour la première fois à les considérer.

III. — Formes quadratiques.

54. Nous allons maintenant dire quelques mots de la représentation des nombres par les formes quadratiques. Nous avons déjà vu que la forme $x^2 + y^2$ peut représenter seulement les nombres dont tous les facteurs premiers impairs sont de la forme $4n + 1$. Il n'est pas en général aussi simple de trouver tous les nombres qui peuvent être représentés par une forme quelconque du second degré : $ax^2 + 2bxy + cy^2$. Nous ne pouvons même, sans dépasser les limites de cet ouvrage, traiter complètement cette question difficile ; nous voulons simplement indiquer les principes fondamentaux sur lesquels repose sa solution.

D'après une remarque faite au début de ce chapitre, nous pouvons nous borner à considérer les représentations *propres* et supposer par conséquent x et y premiers entre eux. Le problème posé est alors le suivant : a, b, c, m étant quatre entiers donnés, peut-on trouver deux nombres x et y premiers entre eux, vérifiant l'égalité

$$ax^2 + 2bxy + cy^2 = m\ ?$$

Nous supposons, suivant l'usage, le coefficient de xy pair ; s'il était impair, il suffirait de multiplier la forme par 2 et de chercher les nombres pairs $2m$ qu'elle peut représenter.

Une première notion très importante est celle des formes équivalentes ; il est clair que si l'on pose

$$(1) \qquad \begin{cases} x = \alpha x' + \beta y', \\ y = \gamma x' + \delta y', \end{cases}$$

on a

$$ax^2 + 2bxy + cy^2 = a'x'^2 + 2b'x'y' + c'y'^2$$

avec

$$a' = a\alpha^2 + 2b\alpha\gamma + c\gamma^2,$$

$$b' = a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta,$$

$$c' = a\beta^2 + 2b\beta\delta + c\delta^2.$$

La forme $f' = a'x'^2 + 2b'x'y' + c'y'^2$ s'appelle la forme *transformée* de $f = ax^2 + 2bxy + cy^2$ *par la substitution* (1), qu'on repré-

sente souvent d'une manière abrégée par le symbole

$$S = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix},$$

et on écrit symboliquement

$$f S = f'.$$

Il est clair que si l'on suppose α, β, γ, δ entiers et si l'on donne des valeurs entières à x', y', il en résulte des valeurs entières pour x, y. Par conséquent, tout nombre qui peut être représenté par f' peut aussi être représenté par f.

Mais la réciproque n'est généralement pas vraie. En effet, si l'on ne fait aucune hypothèse particulière avec α, β, γ, δ, les formules (1) peuvent bien en général être résolues par rapport à x', y', mais les valeurs ainsi obtenues,

$$(2) \quad \begin{cases} x' = \dfrac{\delta x - \beta y}{\alpha\delta - \beta\gamma}, \\ y' = \dfrac{\alpha y - \gamma x}{\alpha\delta - \beta\gamma}, \end{cases}$$

ne font pas toujours correspondre à des valeurs entières de x et de y, des valeurs entières de x', y'.

On voit même que pour que x', y' soient certainement entiers quand x et y le sont, on doit supposer

$$(\alpha\delta - \beta\gamma)^2 = 1.$$

Lorsque cette condition sera vérifiée, les deux formes f et f' seront dites *équivalentes.* Tout nombre représenté par l'une d'elles peut aussi être représenté par l'autre ; connaissant les valeurs des variables qui correspondent à la première de ces représentations, on pourra, à l'aide des formules (1) ou (2), calculer les valeurs qui correspondent à la seconde.

Remarquons que l'on peut avoir, soit

$$\alpha\delta - \beta\gamma = +1,$$

soit

$$\alpha\delta - \beta\gamma = -1.$$

Dans le premier cas, les deux formes sont dites *proprement équivalentes ;* dans le second cas, *improprement équivalentes.*

Les substitutions correspondantes sont respectivement dites propres et impropres.

On voit l'intérêt que présente la question de l'équivalence des for-

mes, au point de vue de la représentation des nombres. Il est facile d'indiquer *une condition nécessaire* pour que deux formes soient équivalentes, il est moins aisé de trouver les conditions nécessaires et suffisantes. Cette condition nécessaire nous est fournie par la propriété d'invariance bien connue que possède le discriminant d'une forme quadratique. On appelle déterminant d'une forme

$$ax^2 + 2bxy + cy^2$$

le discriminant changé de signe :

$$D = b^2 - ac.$$

On sait que si l'on remplace les variables x et y par d'autres variables x', y' au moyen d'une substitution

$$x = \alpha x' + \beta y',$$
$$y = \gamma x' + \delta y',$$

on a

$$D' = b'^2 - a'c' = (b^2 - ac)(\alpha\delta - \beta\gamma)^2,$$

en désignant par a', b', c' les coefficients de la forme en x', y'. Si, en particulier, elle est équivalente à la forme donnée, on a

$$(\alpha\delta - \beta\gamma)^2 = 1$$

et par suite

$$b'^2 - a'c' = b^2 - ac.$$

Deux formes équivalentes ont des déterminants égaux ; il est aisé de s'assurer que la réciproque n'est pas toujours vraie, c'est-à-dire que deux formes peuvent avoir des déterminants égaux sans être équivalentes.

55. Ce qui donne surtout de l'importance à la théorie de l'équivalence, c'est ce fait que nous allons mettre en évidence : *pour rechercher si un nombre peut être représenté par une forme, il suffit de savoir reconnaître si deux formes sont équivalentes ; pour trouver effectivement les nombres qui réalisent la représentation, il suffit de savoir trouver les substitutions qui permettent de passer d'une forme donnée à une autre forme équivalente également donnée.*

Soit en effet

$$m = a\xi^2 + 2b\xi\eta + c\eta^2$$

une représentation propre du nombre m par la forme

$$ax^2 + 2bxy + cy^2 ;$$

ξ, η sont donc supposés premiers entre eux. Il sera par conséquent possible de trouver deux nombres ξ', η' vérifiant l'égalité

$$\xi\eta' - \eta\xi' = 1.$$

Cela posé, considérons la substitution (*)

$$\begin{pmatrix} \xi & \xi' \\ \eta & \eta' \end{pmatrix}.$$

Elle transforme visiblement la forme proposée en la forme équivalente

$$mx'^2 + 2nx'y' + py'^2.$$

Si nous désignons par D le déterminant $b^2 - ac$ de la forme proposée, on a

$$n^2 - mp = D.$$

On en conclut

$$n^2 \equiv D \qquad (\text{mod. } m).$$

Or n est un nombre entier, donc D doit être résidu quadratique de m ; ou plutôt, tout nombre m, pouvant être représenté par une forme, doit être tel que le déterminant de la forme soit résidu quadratique par rapport à ce nombre. On voit l'importance du problème que nous avons résolu à la fin du chapitre précédent, à l'aide de la loi de réciprocité ; nous obtenons immédiatement une condition nécessaire pour la représentation.

Cette condition est-elle suffisante ? Supposons-la vérifiée ; nous pourrons déterminer n par la congruence

$$n^2 \equiv D \qquad (\text{mod. } m)$$

et ensuite p par l'équation

$$p = \frac{n^2 - D}{m},$$

qui fournira une valeur entière ; il faudra alors reconnaitre si la forme

$$mx^2 + 2nxy + py^2$$

est équivalente à la forme proposée et, dans le cas de l'affirmative, pour avoir ξ ou η, trouver la ou les substitutions qui permettent de passer de l'une à l'autre. Nous n'examinerons pas en détail ces problèmes ; nous ne pourrions le faire sans sortir du cadre que nous

(*) On peut remarquer que c'est une substitution *propre* ; on en conclura que l'on peut substituer dans l'énoncé précédent et dans ce qui suit : *proprement équivalent* à : *équivalent*.

nous sommes imposé ; indiquons seulement qu'on sait toujours les résoudre au moyen d'un nombre fini d'opérations.

Nous laissons au lecteur le soin de démontrer qu'en prenant pour n deux solutions de la congruence

$$n^2 \equiv D \qquad (\text{mod. } m),$$

congrues entre elles (mod. m), on n'obtient pas des résultats différents ; on obtiendra donc toutes les solutions possibles en prenant pour n les $\psi(m)$ solutions incongrues entre elles (mod. m).

ALGÈBRE SUPÉRIEURE

DEUXIÈME PARTIE

ALGÈBRE SUPÉRIEURE

CHAPITRE PREMIER

L'ALGÈBRE ÉLÉMENTAIRE

I. — Nombres entiers positifs.

1. Nous nous proposons d'exposer dans les leçons qui suivent la théorie des équations algébriques telle qu'elle a été, à la suite des recherches de Gauss et d'Abel, édifiée par Galois ; mais, afin de pouvoir aborder et présenter cette théorie avec toute la netteté désirable, il nous a paru nécessaire de reprendre à ses débuts l'algèbre élémentaire pour préciser autant que possible quelques-unes des notions acquises, et donner aux termes que l'on emploiera dans la suite leur vraie valeur.

Nous partirons donc de la définition donnée d'abord pour les nombres entiers positifs : on constate qu'avec des objets isolés, qu'on regarde comme identiques, ce qui veut dire qu'on ne porte point l'attention sur les différences qui existent entre eux, il est possible de former des *systèmes* ou *groupements différents*, dans lesquels on regarde tous les objets comme jouant le même rôle. Ces groupements considérés successivement en allant du simple au composé sont dits formés par la réunion de *une*, *deux*, *trois*,... *unités*, en désignant d'une manière générale par le mot *unité* l'objet choisi, quelle que soit sa nature.

Pour étudier les rapports de ces groupements entre eux, il a été indispensable de désigner chacun d'eux par un nom et de le représenter par un signe. Les nombres entiers positifs sont précisément les signes ou les noms qu'on a choisis pour cela. Ce sont donc uniquement des *symboles* par lesquels on représente les systèmes d'unités dont on vient de parler.

Le nombre *zéro*, introduit pour la commodité du langage, est également un symbole qui représente simplement l'absence de tout objet de l'espèce considérée, c'est-à-dire l'absence de toute *unité*.

Si l'on examine maintenant, *au point de vue de leur constitution*, les divers systèmes que l'on vient de définir, on s'aperçoit qu'ils ont entre eux des relations très simples. Chacun d'eux, par exemple, peut s'obtenir en réunissant le précédent avec le système composé d'une unité, et cette propriété est souvent donnée comme un moyen de construire tous les systèmes, dans l'ordre où nous les avons considérés, en partant d'une unité ; de même le système représenté par le nombre 3 s'obtient en supprimant dans le système représenté par 5 un système représenté par 2, etc., etc.

Il existe donc des *modes de composition* de ces systèmes, c'est-à-dire *des moyens de passer de deux d'entre eux à un troisième*. Le plus simple de ces modes consiste dans la réunion de deux systèmes pour en former un seul ; on l'appelle *réunion* ou *addition* des systèmes. Le système qui résulte de la réunion de deux systèmes s'appelle leur *somme*. Nous allons montrer ici que le calcul des nombres entiers positifs, tel qu'on l'entend dans les éléments, n'est qu'un développement *purement logique* des propriétés de l'addition, établies par *l'étude directe des systèmes d'unités*. Ajoutons d'abord, *pour définir la manière de parler consacrée par l'usage*, que l'on convient d'employer pour les symboles qui représentent les systèmes d'unités, c'est-à-dire pour les entiers positifs, le même langage que pour ces systèmes eux-mêmes. Au lieu de dire : le système représenté par le nombre 7 est la somme des systèmes représentés par les nombres 3 et 4, on dira simplement : le nombre 7 est la somme des nombres 3 et 4. Pour éviter même l'emploi d'une phrase, on écrit

$$7 = (3 + 4),$$

l'expression $(3+4)$ représentant la somme des nombres 3 et 4 et le signe $=$ indiquant l'*identité* des symboles qu'il sépare.

2. Passons maintenant aux propriétés fondamentales de l'addition des entiers positifs, *auxquelles on arrive, comme il a été dit, par l'étude directe des systèmes d'unités* (*).

1° Si l'on définit la somme de trois entiers a, b, c par l'égalité

$$a+b+c=(a+b)+c,$$

dans laquelle $(a+b)$ indique la somme des nombres a et b, on a également

$$a+b+c=a+(b+c),$$

ce qu'on énonce en disant : *L'addition des entiers est associative.*

2° Soient a, b deux entiers positifs ; on a $(a+b)=(b+a)$; en d'autres termes : *L'addition des entiers est commutative.*

3° *L'addition du symbole zéro est une addition d'effet nul*, c'est-à-dire que l'on a $(a+0)=a$, quel que soit l'entier positif a.

4° *Si à un nombre a on ajoute des nombres différant entre eux on obtient encore des nombres différant entre eux.* On peut donc conclure des égalités

$$(a+b)=d,$$
$$(a+c)=d,$$

la nouvelle égalité $b=c$. Il résulte de là que l'addition de zéro est la seule opération d'effet nul.

Les quatre propriétés précédentes suffisent pour développer le calcul des nombres entiers positifs ; c'est ce que nous allons constater.

Tout d'abord, *pour la commodité de l'écriture*, a étant un entier positif, on a représenté les sommes a, $a+a$, $a+a+a$, etc. par les nouveaux symboles $a.1$, $a.2$, $a.3$, etc.

On dit que ces symboles $a.1$, $a.2$, $a.3$, etc. définissent un nouveau mode de composition des entiers a et 1, a et 2, a et 3, etc... la composition par *multiplication*. Il est bien clair qu'il n'y a pas là, *en ce moment*, un mode de composition vraiment nouveau, mais seulement une notation commode.

Les relations des symboles de la forme $a.b$ entre eux, c'est-à-dire les *propriétés fondamentales de la multiplication*, s'établissent

(*) Il est bien évident qu'on pourrait se donner *a priori* ces propriétés, définir par là l'addition et constituer un ensemble de symboles déduits de l'un d'eux par addition répétée de ce symbole avec lui-même ; on éviterait ainsi l'introduction des systèmes d'unités.

aisément *en partant de la définition même des nouveaux symboles.* Nous les énonçons ci-dessous

La multiplication des entiers est :

1° *Associative ;*

2° *Commutative ;*

3° *Distributive par rapport à l'addition ;*

ce qui se traduit par les égalités :

$$(a.b).c = a.(b.c),$$

$$(a.b) = (b.a),$$

$$(a+b).c = (a.c + b.c);$$

4° *La multiplication par 1 est, par définition, une opération d'effet nul ;*

5° *Les égalités*

$$(a.b) = d,$$

$$(a.c) = d,$$

permettent d'écrire $b = c$; cela résulte de la définition même des premiers membres. On déduit de là ce fait que la multiplication par 1 est la seule opération d'effet nul.

Nous n'avons pas défini jusqu'à présent les expressions $a.2$, $a.3$. ... dans le cas où a est le nombre zéro. On peut étendre à ce cas la définition donnée lorsque a est quelconque et l'on reconnait alors que $(0.b) = 0$ quel que soit b. On convient alors d'écrire également $(b.0) = 0$ en étendant la propriété commutative de la multiplication à ce cas. La convention est légitime, car le produit $(b.0)$ n'a aucun sens jusqu'à présent d'après la définition donnée de la multiplication des entiers.

Remarquons que cette convention montre que la propriété de la multiplication d'être distributive par rapport à l'addition se conserve pour l'ensemble des entiers positifs et du nombre zéro.

On a en effet

$$b.(a+0) = b.a + b.0 = b.a,$$

$$(a+0).b = a.b + 0.b = a.b,$$

et il apparait immédiatement qu'on aurait pu définir $b.0$ et $0.b$ en étendant à l'ensemble des entiers positifs et de zéro la propriété distributive de la multiplication, sans même supposer la commutativité.

A quelque point de vue que l'on se place, on peut donc énoncer la proposition suivante : *le produit d'un entier quelconque par zéro est encore zéro.* La définition donnée du produit ($a.b$) montre d'ailleurs que ce produit n'est zéro que si a ou b sont eux-mêmes zéro.

De même que l'on a représenté par $a.1$, $a.2$, $a.3$, etc. les sommes a, $a+a$, $a+a+a$, etc., il est commode d'introduire une nouvelle notation pour représenter les produits a, $a.a$, $a.a.a$, etc. On écrit ces produits a^1, a^2, a^3, etc. Si l'on considère le symbole a^b ainsi défini, il est clair qu'on peut le regarder comme résultant d'un certain mode de composition des nombres a et b ; c'est ce mode qu'on appelle *élévation aux puissances.* On peut d'ailleurs ajouter, comme pour la multiplication, que ce n'est pas ici un mode vraiment nouveau, mais simplement une nouvelle notation. Les lois qui gouvernent le calcul du symbole a^b s'établissent en partant de sa définition, d'une façon immédiate.

On a d'abord les formules

$$a^b.a^c = a^{b+c},$$

$$(a^b)^c = a^{b.c}.$$

Ajoutons qu'il existe comme dans les modes de composition précédents une opération d'effet nul, l'élévation à la puissance 1.

Il résulte d'ailleurs de la définition même de a^b que l'on n'a

$$a^b = a^{b'}$$

que si

$$b = b',$$

d'où l'on conclut qu'il n'y a qu'une seule opération d'effet nul.

Enfin si l'on convient d'étendre au cas où l'un des exposants est nul les lois qui gouvernent l'élévation aux puissances, on aura

$$a^b.a^0 = a^{b+0} = a^b,$$

ce qui définit a^0 comme égal à 1 quel que soit l'entier a. Nous n'insisterons pas ici sur ce sujet, l'élévation aux puissances ne jouant pas, *dans ce qu'on appelle d'habitude l'Algèbre*, un rôle comparable comme importance aux deux modes de composition précédemment indiqués.

Remarquons cependant, en passant, qu'il serait possible de continuer dans la voie où nous nous sommes engagés et qu'il serait par exemple *utile* d'introduire une nouvelle notation pour représenter

les nombres a^b, a^{b^b}, $a^{b^{b^b}}$, etc. en mettant en évidence le rôle qu'y jouent a, b et le *nombre* m *des exposants* b *superposés*. On pourrait continuer ainsi indéfiniment, mais tout cela est du ressort de l'étude des symboles dits *transcendants* ; nous ne nous en occupons pas dans ces leçons, qui seront pour ainsi dire uniquement consacrées à l'étude des deux premiers modes.

II. — Nombres entiers négatifs.

3. En considérant les entiers positifs nous porterons maintenant notre attention uniquement sur ce fait que ce sont des *symboles connus*, dont on connaît un mode de composition, l'addition, et les lois qui le régissent.

En disant que ces symboles sont *connus*, nous voulons dire que *lorsqu'on a donné un nom à chacun d'eux, par exemple en suivant les règles de la numération décimale, on sait quel est le symbole qui est la somme de deux symboles donnés*. On connaît également d'après la manière dont on a déduit la définition du produit $a.b$ de la définition d'une somme, le produit $(a.b)$ lorsqu'on connaît les facteurs a et b.

En d'autres termes, on peut construire une table carrée d'addition et une table carrée de multiplication pour les entiers positifs ; la seconde lorsqu'on considère seulement un nombre limité de ces entiers est une table de Pythagore ordinaire. On pourrait également construire une table d'élévation aux puissances à double entrée comme les premières, les *exposants* étant sur une ligne horizontale et les *bases* étant sur une ligne verticale, mais comme nous l'avons fait observer, nous considérerons *uniquement*, en Algèbre, l'élévation aux puissances comme une simple notation et non comme un mode de composition nouveau.

La construction de ces tables est *nécessaire et suffisante pour effectuer le calcul des entiers positifs*, en ce sens qu'elle permet de trouver l'entier qu'on obtient en effectuant sur un entier donné un nombre limité des opérations : addition, multiplication, élévation aux puissances. Nous verrons plus loin que ces tables permettent, *théoriquement du moins*, de résoudre tous les problèmes qu'on peut poser sur les entiers positifs *lorsque ces problèmes admettent pour solutions des entiers positifs*.

Par exemple, soit proposé de rechercher l'entier positif, s'il en existe un, qui mis à la place de x satisfait à la relation $a+x=b$, a et b étant des entiers positifs donnés. On consultera dans la table d'addition la ligne qui donne les sommes de l'entier a avec un nombre positif quelconque ; si l'entier b figure dans cette ligne, la colonne dans laquelle il se trouve donnera à son origine le nombre entier cherché. Cette opération s'appellera la résolution de l'équation $a+x=b$ en entiers positifs.

Sinon, il n'existe aucun entier positif x tel que $a+x=b$. Ainsi, il n'existe aucun entier positif qui mis à la place de x vérifie la relation

$$a+x=0,$$

quel que soit l'entier positif a.

4. Nous avons vu précédemment qu'un système de symboles est *connu vis-à-vis de certains modes de composition de ces symboles*, lorsqu'après avoir donné un nom à chaque symbole du système, on connaît le nom du symbole résultant de la composition de deux symboles donnés par l'un des modes spécifiés ci-dessus. Ainsi, dès qu'on a construit une table d'addition, de multiplication et d'élévation aux puissances des entiers positifs, le système de ces entiers est *connu* vis-à-vis des trois modes précédents. Il résulte de là que si l'on adjoint à un ensemble de symboles *connu* de nouveaux symboles auxquels on a donné des noms, le nouvel ensemble sera connu relativement aux mêmes modes de composition, dès qu'on connaîtra les résultats de la composition des nouveaux symboles entre eux ou avec les anciens suivant les modes considérés. C'est cette remarque que nous allons appliquer pour arriver à *connaître* l'ensemble des entiers positifs et négatifs.

Ajoutons que nous appelons ici *composition des symboles*, toute opération qui de deux symboles donnés conduit suivant des règles bien déterminées à un troisième symbole. Nous verrons qu'il est toujours possible de trouver, *et d'un grand nombre de manières différentes*, des éléments *géométriques*, *mécaniques* ou *physiques* qui, *considérés à certains points de vue*, peuvent être représentés par les symboles que nous introduirons ; la composition des symboles sera alors l'image d'une composition effective de ces éléments entre eux. Nous en avons déjà trouvé un exemple dans la multiplication et

l'élévation aux puissances des entiers positifs qui reproduisent des modes de composition des systèmes d'unités faciles à donner.

Nous présenterons d'abord la théorie des entiers négatifs à un point de vue *purement logique*, en mettant en évidence les hypothèses essentielles de cette théorie ; nous justifierons ensuite l'introduction de ces symboles dans les mathématiques, en donnant des exemples d'*éléments* (ou d'opérations portant sur des éléments convenablement choisis) pour lesquels on peut :

1° Etablir une correspondance univoque et réciproque entre les éléments et les entiers positifs et négatifs ;

2° Définir les modes de composition de ces éléments qui suivent les mêmes lois que les modes de composition des entiers positifs et négatifs entre eux.

Tout ceci sera d'ailleurs précisé bientôt.

Considérons la relation $1+x=0$, qui n'est satisfaite pour aucun des symboles connus (entiers positifs) mis à la place de x. Nous ajouterons à l'ensemble des entiers positifs un nouveau symbole qui, *par définition*, vérifiera cette relation ; nous supposerons d'abord que dans la relation $1+x=0$ le signe $+$ indique un mode de composition *déterminé* des symboles 1 et x, mais quelconque, c'est-à-dire qui n'est pas nécessairement identique à l'addition déjà définie des entiers positifs. Il est toujours légitime de continuer à appeler *addition* cette composition, tout en spécifiant que l'addition des entiers positifs doit être distinguée de celle-là.

Il est clair que *si l'on ne dit rien sur le mode de composition de* 1 *et x représenté ici par le signe $+$, on ne peut également rien dire sur le calcul du symbole x.*

Les expressions $a+x$ et $a.x$, où a est un nombre entier positif, ne sont, par exemple, aucunement définies, et il en est de même de $x.x$. De l'égalité $(1+x)=0$ on ne peut en effet déduire que les égalités

$$a+(1+x)=a, \quad a \text{ étant un entier quelconque,}$$

et

$$(1+x).a=0,$$

qui montrent que le symbole $(1+x)$ se comporte absolument comme le symbole zéro vis-à-vis des entiers positifs ; c'est d'ailleurs la définition qu'on en a donnée.

Nous supposerons que le symbole x se compose avec le symbole 1 pour donner zéro, *en suivant les lois fondamentales de l'ad-*

dition des nombres entiers positifs. Je dis que cette hypothèse permettra le calcul du symbole x, calcul qu'on pourra dès lors considérer comme connu vis-à-vis de l'addition.

D'abord la propriété de l'addition énoncée en quatrième lieu montre que le symbole x défini par $(1+x)=0$ est *unique*. La commutativité prouve qu'on peut écrire

$$(1+x)=1+x=(x+1)=0.$$

Enfin on a, puisque l'addition est associative,

$$a+(1+x)=(a+1)+x=a,$$

c'est-à-dire que l'addition d'un entier positif quelconque $a+1$ et du symbole x est définie, la somme obtenue étant a.

Les égalités

$$(a+1)+x=a,$$
$$(b+1)+x=b,$$
$$\ldots\ldots\ldots$$

donnent d'ailleurs

$$(a+b+2)+x+x=a+b, \quad \text{etc...},$$

ce qui définit le *calcul additif* des symboles $x+x$, $x+x+x$,... ce calcul étant connu lorsqu'on sait trouver la somme de ces symboles avec des entiers positifs quelconques ou avec eux-mêmes.

Si l'on convient de conserver les mêmes notations pour représenter les sommes $x+x$, $x+x+x$,... que celles introduites pour les entiers positifs, c'est-à-dire de poser par définition :

$$x.1=x,$$
$$x.2=x+x,$$
$$x.3=x+x+x, \quad \text{etc...},$$

on sait ce que représente $x.a$, a étant un entier positif quelconque.

On peut remarquer que ce symbole $x.a$ vérifie l'équation

$$a+x.a=0.$$

Si l'on veut maintenant définir de la manière la plus simple les expressions $a.x$ et $x.x$, on sera amené ici à *supposer* qu'il existe entre le nouveau symbole x et les anciens ou ce symbole x lui-même, un mode de composition qui possède les cinq propriétés fondamentales de la multiplication des entiers positifs.

La commutativité de la multiplication donnera

$$a.x = x.a.$$

Enfin, pour obtenir $x.x$ il suffira de multiplier par x les deux membres de l'équation de définition $1 + x = 0$. On aura, à cause de la distributivité par rapport à l'addition,

$$x.(1 + x) = x + x.x = 0$$

ou, en ajoutant le nombre 1 aux deux membres : $x.x = 1$.

On continuerait de même pour obtenir les expressions x^m, où m est un entier positif.

Remarquons ici que si l'on voulait introduire dans le calcul les expressions a^x et x^x, il faudrait donner un sens à ces symboles qui n'en ont pas jusqu'à présent. On *supposerait* alors l'existence d'un troisième mode de composition de a et x ou de x avec lui-même possédant les propriétés de l'élévation aux puissances. C'est ce qu'on fait effectivement en Analyse, mais, comme nous l'avons déjà dit, dès que l'exposant b de la puissance n'est pas un entier positif, l'étude du symbole a^b ne fait pas partie de l'Algèbre.

En résumé, en faisant sur le symbole x, qu'on introduit, l'hypothèse qu'il se combine avec les entiers positifs et avec lui-même suivant deux modes différents : l'un possédant les quatre propriétés fondamentales de l'addition, l'autre les cinq propriétés fondamentales de la multiplication, on peut affirmer que la relation $1 + x = 0$ suffit à définir le calcul de x d'une manière unique et bien déterminée relativement aux deux modes de composition : addition et multiplication.

On peut remarquer qu'avec le symbole x sont introduits tous les symboles de la forme $a.x$, et la relation $x.x = 1$ permet d'affirmer que ce sont les seuls qu'on introduira ainsi.

On donne aux symboles $a.x$ ou $x.a$ le nom de *nombres entiers négatifs* et on représente le symbole x, défini comme nous l'avons dit, à l'aide de $1 + x = 0$, par le signe (-1), qu'on énonce : *moins un*. Les symboles $x.a$ sont alors représentés par le signe $(-1).a$. Pour simplifier les écritures, *il est commode* d'écrire simplement $(-a)$ au lieu de $(-1).a$ ou même $-a$; cela ne peut prêter à aucune ambiguïté, le signe $-$ n'ayant pas de sens pour nous jusqu'à présent.

5. Il est possible de présenter les opérations qui précèdent d'une façon plus nette encore.

Lorsque des objets bien définis forment un ensemble possédant les propriétés suivantes :

1° *De deux objets de l'ensemble on peut déduire d'une manière bien déterminée un troisième objet du même ensemble ;*

2° *La composition des objets considérée est associative;*

3° *Un même objet associé à des objets différents conduit par cette composition à des objets différents ;*

on dit que les objets constituent un groupe.

Le groupe est dit *limité* ou *illimité* suivant qu'il est possible on non d'épuiser l'ensemble en prenant successivement et dans un certain ordre tous les objets différents qui en font partie.

La définition précédente étant donnée, on remarque immédiatement que tous les entiers positifs (y compris zéro) constituent un groupe illimité lorsqu'on envisage leur composition par addition. Si l'on exclut le symbole zéro, qui joue un rôle *singulier* dans la multiplication, on peut également dire que les nombres 1, 2, 3, ... forment un groupe illimité, la composition des éléments étant la multiplication.

Ces deux groupes ont une constitution très simple :

Tous les éléments du premier *sauf zéro* dérivent en effet de l'élément désigné par 1 par addition répétée de cet élément avec lui-même.

Tous les éléments du second dérivent uniquement des éléments dits *nombres premiers*, c'est-à-dire s'obtiennent en multipliant entre eux les nombres premiers; c'est ce qu'a établi du moins la théorie de la divisibilité.

Nous dirons qu'un groupe est *connu* lorsque, deux éléments du groupe étant donnés, il est possible de donner l'élément qui en résulte par la composition correspondante. On peut, lorsqu'un groupe est connu, former une table de composition de ses éléments, table nécessairement à double entrée, qu'on appelle *table de structure* du groupe, et il est clair que, si l'on a construit cette table de structure, le groupe est connu. Dans le cas des entiers positifs, ces tables de structure sont les tables d'addition et de multiplication dont nous avons parlé; en les étudiant on retrouverait aisément les propriétés fondamentales de la composition qui ont servi à les construire.

Etant donné un groupe d'objets, vis-à-vis d'un certain mode de composition de ces objets, on peut se proposer d'*étendre* ce groupe de façon à ce qu'il renferme un nouvel objet ; d'une manière plus précise on peut se proposer de définir un nouvel ensemble d'objets :

1° Qui renferme au moins les objets du groupe donné et le nouvel objet ;

2° Qui possède les propriétés du groupe relativement à un certain mode de composition des objets, le mode considéré se réduisant au premier lorsque les objets à composer appartiennent au groupe donné.

Il est bien évident que pour former ce nouvel ensemble on devra, en général, ajouter plus d'un objet au groupe. On peut remarquer en outre que le nouveau groupe sera connu lorsqu'on aura construit sa table de structure, c'est-à-dire donné les résultats de la composition des nouveaux objets avec les anciens et des nouveaux objets entre eux, suivant le mode considéré.

Il suffit de se rappeler comment nous avons introduit les entiers négatifs pour voir immédiatement que c'est précisément ce problème que nous avons résolu. Nous avons en effet constitué par l'ensemble des entiers positifs et négatifs un nouveau groupe, la composition des éléments étant l'addition des entiers, ou, lorsqu'on exclut zéro, leur multiplication.

Lorsqu'on considère la table de structure d'un groupe, on constate en général que toutes les relations qu'elle conduit à écrire entre ses éléments sont des conséquences nécessaires d'un nombre limité d'entre elles, qu'on appelle *relations fondamentales*, et des lois de la composition. Pour introduire les entiers négatifs nous avons ajouté, pour définir le calcul additif, un élément (-1) et une relation fondamentale : $1 + (-1) = 0$, de laquelle la table de structure du groupe peut se déduire en appliquant les lois de l'addition supposées conservées. Lorsqu'il s'est agi de définir le calcul multiplicatif, il a suffi alors de supposer conservées les propriétés fondamentales de la multiplication : commutativité et distributivité.

A l'égard des groupes formés par les entiers positifs et négatifs, composés par addition ou par multiplication, on remarque que les opérations considérées étant commutatives, la table de structure sera symétrique par rapport à une diagonale. De tels groupes sont dits *groupes abéliens*.

6. Nous venons d'introduire dans le calcul, à un point de vue *purement logique*, les entiers négatifs ; nous allons montrer l'utilité de cette introduction, c'est-à-dire *légitimer pratiquement l'étude de ces symboles*, en donnant des exemples d'éléments (ou d'opérations portant sur des éléments déterminés) pour lesquels on peut définir un mode de composition possédant les propriétés de l'addition, un autre mode possédant les propriétés de la multiplication, et établir une correspondance *univoque et réciproque* avec les entiers positifs et négatifs. D'une façon plus précise :

1° A chaque élément correspondra un entier et un seul et réciproquement ;

2° A des éléments différents correspondront des entiers différents ;

3° A la somme et au produit de deux éléments correspondront respectivement la somme et le produit des entiers correspondants.

Parmi ces exemples, l'un des plus simples nous est donné par la Géométrie. Considérons une droite indéfinie sur laquelle nous supposons fixé un sens de parcours que nous appellerons sens positif; nous prenons sur cette droite un *segment* déterminé OA parcouru dans le sens positif. Nous convenons de considérer comme équivalents, c'est-à-dire de représenter par le même symbole deux segments de même longueur et de même sens, quelle que soit leur position sur la droite.

Nous ferons correspondre le segment OA à l'entier 1, le même segment décrit en sens inverse à l'entier -1. Si nous définissons alors *la somme de deux segments comme le segment qui a pour origine l'origine du premier et pour extrémité l'extrémité du second, après qu'on a fait coïncider l'origine du second avec l'extrémité du premier*, on voit que la correspondance annoncée entre les segments ainsi construits à l'aide du segment OA parcouru dans un sens et dans l'autre et les entiers positifs ou négatifs est assurée.

Le calcul additif des segments est alors identique à celui des entiers.

Si maintenant on définit *le produit de deux segments comme un segment composé avec l'un d'eux comme l'autre est composé avec le segment* OA, on a défini une multiplication des segments qui représente celle des entiers.

On peut remarquer que le segment correspondant à zéro est celui dont l'origine et l'extrémité coïncident.

III. — Nombres fractionnaires.

7. L'introduction des nombres fractionnaires se fait suivant les mêmes principes que celle des entiers négatifs.

Nous partons de la relation $a.x = 1$, où a est un entier positif ou négatif, mais différent de ± 1 et de zéro. Dans le cas où $a = \pm 1$, il existe en effet un symbole entier ± 1 qui vérifie la relation $a.x = 1$; dans le cas $a = 0$ il n'existe aucun entier

qui mis à la place de x vérifie $a.x = 1$; *nous écarterons ce dernier cas de nos considérations à cause du rôle singulier que joue zéro dans la multiplication.*

Soit donc la relation $a.x = 1$, a étant choisi comme il a été dit ; il n'existe aucun entier qui mis à la place de x vérifie cette relation. Nous introduirons alors un nouveau symbole x qui, par définition, est tel que l'on ait $a.x = 1$, c'est-à-dire qu'il existe un mode de composition du symbole x et du symbole a, mode que nous appellerons multiplication, et qui conduit au nombre 1.

Pour permettre le calcul du symbole x, c'est-à-dire former des tables d'addition et de multiplication du symbole x avec lui-même et avec les symboles déjà connus, nous supposerons d'abord qu'il se compose avec lui-même et avec les entiers suivant un mode possédant les propriétés fondamentales de la multiplication. Nous exceptons bien entendu la propriété *distributive*, puisque nous n'admettons d'abord qu'un seul mode de composition.

On peut conclure de cette hypothèse qu'il existe un seul symbole x tel que l'on ait $(a.x) = 1$ et l'on peut définir le produit de ce symbole par un entier quelconque b, à l'aide de la suite d'égalités

$$b.(a.x) = (b.a).x = (a.b).x = a.(b.x) = b.$$

On aura de même

$$(a.x).(a.x) = a.x.a.x = (a.a).(x.x) = 1,$$

ce qui donne $a^2.x^2 = 1$, en adoptant la notation $x.x = x^2$.

On peut donc calculer x^m lorsque m est un entier positif.

Supposons maintenant l'existence d'un second mode de composition du symbole x avec lui-même ou les entiers, possédant les propriétés fondamentales de l'addition, la multiplication étant distributive par rapport à ce mode. Si l'on conserve le signe $+$ pour indiquer ce mode de composition, de la relation $(a.x) = 1$ on peut déduire

$$(a.x) + (a.x) = a.(x + x) = 2,$$

ce qui définit $x + x$ d'une manière unique. La définition montre d'ailleurs que l'on a

$$x + x = x.2 = 2.x,$$

puisque

$$a.(2.x) = 2.(a.x) = 2,$$

c'est-à-dire que le symbole $x+x$ coïncide avec un symbole déjà connu.

On verrait également que la relation

$$(a.x)+(a.b)=a.(x+b)$$

définit le symbole $(x+b)$. Il résulte de là que l'on sait composer le symbole x soit avec lui-même, soit avec les entiers par voie d'addition ou de multiplication ; en d'autres termes, le *calcul* du symbole x est connu. On peut remarquer que l'on a toujours $x.0=0.x=0$, c'est-à-dire que la multiplication par zéro reste singulière.

L'ensemble des symboles $b.x^m+c$, où b, c sont des entiers quelconques et m un entier positif, renferme tous les symboles déduits de x par les modes de composition précités. On peut dire que cet ensemble constitue un *groupe illimité* d'éléments, soit au point de vue de la composition additive, soit au point de vue de la multiplication. *Les relations fondamentales de ce groupe dérivent toutes des lois qui régissent ces modes de composition et de la relation fondamentale* $(a.x)=1$ *qui définit* x.

Il est commode d'introduire directement le symbole x dans le calcul et d'abandonner alors la relation fondamentale qui le définit ; on le fait en donnant un nom à ce symbole. On l'appelle *inverse de* a et on le représente par un signe qui rappelle son origine : $\left(\frac{1}{a}\right)$; on a alors par définition $a.\left(\frac{1}{a}\right)=1$. Nous appellerons cela *expliciter* le symbole ; c'est en effet *donner un signe explicite pour représenter un élément défini par une relation implicite.* C'est l'opération déjà faite lorsqu'on a désigné par $(-a)$ le symbole qui vérifie $x+a=0$, a étant entier positif.

Pour simplifier les écritures on écrit souvent $b.\left(\frac{1}{a}\right)=\frac{b}{a}$; cela ne présente évidemment aucun inconvénient, $\frac{b}{a}$ n'ayant jusqu'à présent aucun sens.

L'entier a n'ayant pas jusqu'alors été fixé, on peut supposer qu'on prenne successivement pour a tous les entiers positifs ou négatifs. On introduira ainsi tous les symboles de la forme $\frac{p}{q}$, où p et q sont deux entiers quelconques ; ce sont ces symboles qu'on appelle

les *nombres rationnels*. Il est à remarquer que tous les symboles ainsi introduits ne sont pas distincts, et que si l'on a

$$p = m.p', \qquad q = m.q',$$

on en déduit

$$\frac{p}{q} = \frac{p'}{q'}.$$

Si l'on veut ne pas introduire de symboles inutiles, il faudra faire l'introduction des symboles *séparément*, c'est-à-dire après avoir introduit le symbole $\frac{1}{2}$, par exemple, n'introduire un nouveau symbole que si la relation qui doit le définir n'est vérifiée pour aucun des symboles déjà introduits. On reconnait immédiatement qu'il est nécessaire et suffisant d'introduire les symboles définis par la relation $p.x = 1$, p étant un nombre premier quelconque, c'est-à-dire les *inverses des nombres premiers*. Cette remarque résulte d'ailleurs de la constitution du groupe formé par les entiers positifs et négatifs vis-à-vis de la multiplication.

8. Si l'on admet pour les nombres rationnels l'existence des deux modes de composition : addition et multiplication, le calcul de ces nombres est complètement défini et connu relativement à ces deux modes.

Par exemple, si l'on a

$$a.x = \alpha,$$
$$b.y = \beta,$$

a, α, b, β étant des entiers quelconques, il en résulte

$$a.b.x = \alpha.b,$$
$$b.a.y = \beta.a,$$

c'est-à-dire

$$(a.b).(x+y) = (\alpha b + \beta a),$$

ce qui définit la somme de deux nombres rationnels x et y :

$$(x+y) = \frac{(\alpha b + \beta a)}{(a.b)}.$$

On aurait de même

$$a.x.b.y = \alpha.\beta$$

ou

$$(a.b).(x.y) = \alpha.\beta,$$

ce qui donne

$$(x.y) = \frac{(\alpha.\beta)}{(a.b)}.$$

Enfin nous pouvons ajouter que si l'on considère une relation de la forme $a.x = b$, où a et b sont des nombres rationnels, il existe un symbole rationnel ou entier et un seul qui mis à la place de x vérifie cette relation. Soient, en effet,

$$\alpha.a = p,$$
$$\beta.b = q$$

les égalités qui définissent a et b ; l'égalité qui définit x peut s'écrire

$$\alpha.\beta.a.x = \alpha.\beta.b$$

ou encore

$$(p.\beta).x = (\alpha.q).$$

On déduit donc de là

$$x = \frac{(\alpha.q)}{(p.\beta)}.$$

D'une manière générale, lorsque dans un ensemble de symboles qui se composent entre eux suivant un mode additif et un mode multiplicatif, il existe :

1° Un et un seul symbole de l'ensemble qui mis à la place de x satisfait à la relation $a + x = b$, a et b étant deux symboles quelconques de l'ensemble, on dit que la *soustraction* est possible dans l'ensemble ;

2° Un et un seul symbole de l'ensemble tel que mis à la place de x il vérifie l'équation $a.x = b$, on dit que la *division* est possible dans l'ensemble.

Les nombres entiers positifs et négatifs forment un ensemble où la soustraction est possible. Si on ajoute les nombres rationnels, on a un ensemble dans lequel la soustraction et la division sont possibles. Le symbole zéro étant singulier dans la multiplication, la division par zéro reste toujours exclue de nos considérations.

Nous n'insistons pas ici sur les définitions de la soustraction et de la division comme opérations inverses de l'addition et de la multiplication, cela n'est pour nous d'aucune importance.

9. Passons maintenant à la légitimation des symboles que nous venons d'introduire ; elle sera complète lorsque nous aurons donné des exemples d'éléments (ou d'opérations portant sur ces éléments) pour lesquels on connaît deux modes de composition possédant l'un les quatre propriétés fondamentales de l'addition, l'autre les cinq propriétés fondamentales de la multiplication et tels que la correspondance entre les éléments et nos symboles soit univoque et réciproque.

Il suffira de choisir ici nos éléments parmi les grandeurs pour lesquelles on a la conception d'une division en parties égales. Nous pourrons conserver l'exemple, donné précédemment, des segments portés sur une droite et définir par exemple le segment correspondant au symbole $\left(\frac{1}{a}\right)$ comme celui qui conduit au segment unité lorsqu'on le compose avec lui-même de la même manière qu'on compose le segment unité avec lui-même pour former le segment correspondant à a. Il suffira de conserver également les définitions déjà données de l'addition et de la multiplication des segments pour que la correspondance entre les segments et nos nombres rationnels soit complète et complètement définie.

A ce propos nous observerons que dans l'exemple précédent tous les nombres rationnels sont représentés ; cela tient à ce qu'on admet la possibilité de diviser un segment *quelconque* en autant de parties égales que l'on veut. Il n'en est pas ainsi en général, c'est-à-dire qu'un système d'objets étant donné pour lesquels on connaît les deux modes de composition : addition et multiplication, il peut se faire que certaines divisions seulement soient possibles ; on ne pourra alors représenter par ces objets qu'une partie des nombres rationnels. C'est ce qui arrive, par exemple, lorsqu'on se propose de diviser un arc de cercle *à l'aide de la règle et du compas seuls ;* on n'obtiendra évidemment ainsi en partant de l'unité que les segments correspondant aux nombres de la forme $\frac{a}{2^n}$, a étant un entier quelconque et n un entier positif.

Cela se présente également lorsqu'on considère des systèmes d'unités A dans lesquels l'unité A est elle-même un système d'autres unités B. Si l'unité A est composée de p unités B, il sera possible de représenter dans le domaine où l'on se place les opérations qui correspondent au calcul additif des fractions de la forme $\frac{a}{p}$ et les multiplications des entiers par ces fractions ; mais il sera impossible de représenter par exemple la multiplication de $\frac{a}{p}$ et $\frac{b}{p}$.

On aperçoit ici la différence essentielle entre une étude d'éléments réels au point de vue de leurs modes de composition et l'étude de symboles possédant ces modes de composition. Alors que la première est sujette à une foule d'irrégularités provenant de l'ensemble d'éléments que l'on considère, irrégularités qu'il faut trouver, la seconde est le développement naturel et logique des hypothèses faites et ne présentera jamais de difficultés.

III. — Polynomes à une variable.

10. On appelle *polynome entier en x de degré m*, toute expression de la forme $a+bx+cx^2+\cdots+lx^m$ dans laquelle $a, b, \ldots l$ sont des nombres rationnels déterminés, positifs ou négatifs, le nombre

l étant différent de zéro, et x un nombre rationnel qu'on laisse *à dessein indéterminé*. Nous appellerons d'une manière générale *variable* un symbole qu'on peut choisir d'une façon arbitraire *dans un ensemble de symboles connus*, et nous dirons que le polynome précédent est un polynome *à une variable x*. Lorsqu'on remplace, dans le polynome, x par un nombre rationnel déterminé, le polynome devient aussi un nombre rationnel déterminé et qu'on sait calculer. Il est facile de voir qu'un polynome *donné* ne peut devenir égal à un nombre rationnel *quelconque* pour un choix convenable du nombre rationnel x; par exemple le polynome à deux termes ou *binome* $x^2 + 1$ ne peut devenir égal ni à zéro, ni à -1, ni à 3, etc. quel que soit le nombre rationnel qu'on mette à la place de x; donc à tous les nombres rationnels le polynome ne fait correspondre que les nombres rationnels d'*une certaine classe*. En algèbre élémentaire, étudier le polynome c'est donner des règles de calcul communes à tous les nombres rationnels de cette classe.

Considérons, par exemple, les deux polynomes

$$P = 2 + 4x - 9x^2,$$

$$Q = 3 - 2x + 5x^3\ ;$$

lorsqu'on fixe le nombre rationnel x, P et Q deviennent des nombres rationnels déterminés. Il est facile de former un polynome qui représente, pour ce même choix de x, la somme de ces nombres rationnels. Il suffit en effet de réunir les termes de P et de Q et de réduire les *termes semblables*, c'est-à-dire renfermant la même puissance de x, en appliquant la propriété distributive de la multiplication. Le polynome ainsi obtenu est

$$R = 5 + 2x - 9x^2 + 5x^3\ ;$$

on l'appelle *somme* des polynomes P et Q, et il est clair que quel que soit le choix fait pour x, le polynome R représentera la somme des nombres rationnels représentés par P et Q.

D'une manière analogue il est facile de former un polynome qui représente, quel que soit le nombre rationnel mis à la place de x, le produit des nombres rationnels représentés par deux polynomes donnés. Si $P = 2 + 3x$, $Q = 3 - 5x$ sont les polynomes donnés, le polynome cherché est

$$R = 6 - x - 15x^2\ ;$$

on l'appelle *produit* des polynomes P et Q.

Dans les deux cas que nous venons de considérer, on a, pour obtenir le polynome R, regardé x comme un symbole se composant avec les nombres rationnels suivant deux modes différents qui possèdent les propriétés fondamentales de l'addition et de la multiplication des nombres rationnels. Le point de vue auquel nous nous plaçons pour considérer les polynomes justifie naturellement ce procédé, puisque x représente pour nous un nombre rationnel indéterminé. Il est bien clair que l'addition et la multiplication des polynomes ainsi définies, possèdent les propriétés fondamentales des mêmes modes de composition entre nombres rationnels ; nous n'y insisterons donc pas.

11. Poursuivant l'analogie que présente l'étude des polynomes et celle des entiers, nous considérerons les relations de la forme

$$P + X = Q$$

et

$$P . X = Q,$$

dans lesquelles P et Q représentent des polynomes donnés et X est un symbole assujetti à vérifier l'une de ces relations et à se composer avec les symboles ordinaires : polynomes entiers, suivant les deux modes si souvent cités.

On voit aisément que la relation $P + X = Q$ définit toujours un polynome entier en x qu'on appelle *différence* des polynomes Q et P *sous la seule condition que les coefficients de* P *et* Q *appartiennent à un ensemble de symboles dans lequel la soustraction est possible.*

Il n'en est pas de même de la relation $P . X = Q$; dans tous les cas on *explicite* le symbole X défini par cette relation en écrivant

$$X = \frac{Q}{P},$$

et on l'appelle *fraction rationnelle.* D'après ce qu'on vient d'affirmer, il peut arriver qu'il existe un polynome entier en x ou un nombre rationnel, qui, mis à la place de X, vérifie la relation donnée $P X = Q$; on dira dans ce cas que la fraction $\frac{Q}{P}$ est *réductible* à un polynome ou à un nombre rationnel; si au contraire cela n'a pas lieu, on a une *véritable fraction.* Des exemples de ces deux cas sont donnés par les relations

$$(x-1).X = (x^2-1), \quad \text{qui donne} \quad X = \frac{x^2-1}{x-1} = x+1$$

et $(x^2+1).X = x^2+x+1$, qui donne $X = \dfrac{x^2+x+1}{x^2+1}$.

Le calcul des symboles de la forme $\frac{Q}{P}$, dans laquelle P et Q sont deux polynomes en x, se déduit immédiatement de leur définition et reproduit par conséquent, *mutatis mutandis*, le calcul des fractions ordinaires $\frac{a}{b}$, a et b étant des entiers; nous n'y insisterons pas non plus.

12. Lorsque a et b sont des entiers positifs, b étant inférieur à a, on sait qu'il existe toujours une identité de la forme $a = b.q + r$ dans laquelle q et r sont également des entiers positifs, r étant inférieur à b; on dit alors que q est le *quotient* et r le *reste* de la division de a par b. L'extension de cette définition aux polynomes va nous permettre d'arriver à des propositions plus importantes : soient A et B deux polynomes entiers en x, le premier de degré m, le second de degré inférieur n; si nous posons l'identité en x

$$A = B.Q + R,$$

Q étant un polynome de degré $m-n$ et R un polynome de degré $(n-1)$, il est possible de déterminer de proche en proche et *d'une manière unique* les coefficients de Q puis ceux de R; parmi ces derniers un certain nombre et même tous peuvent se réduire à zéro. Le polynome Q est appelé *quotient* et le polynome R *reste* de la division de A par B.

Il est presque inutile de remarquer que dans le cas où les coefficients de R sont tous *zéro*, le polynome Q qu'on détermine ainsi est celui auquel se réduit la fraction $\frac{A}{B}$ introduite précédemment. Ajoutons qu'on dit, dans ce cas, que le polynome A est *divisible* par le polynome B ou bien que B est un *diviseur* de A. Nous n'insisterons pas ici sur les *moyens pratiques* employés pour déterminer les coefficients des polynomes Q et R dans le cas général; ce qu'il importe de fixer, c'est que si l'on ordonne les polynomes A, B et Q suivant les puissances décroissantes de x, on aura les coefficients de Q par des relations de la forme $ax = b$, dans lesquelles x est

un coefficient inconnu et a le coefficient *du premier terme de* B. On n'aura donc à effectuer que des divisions par ce coefficient a. Les coefficients de R seront ensuite obtenus par des équations de la forme $\alpha + x = \beta$, α et β étant connus et x étant le coefficient inconnu.

Il résulte de là que *si les coefficients des polynomes* A *et* B *font partie d'un ensemble de symboles dans lequel la division par le coefficient du premier terme de* B *et la soustraction sont possibles, on pourra affirmer l'existence d'une identité de la forme*

$$A = B.Q + R,$$

les coefficients des polynomes Q *et* R *appartenant au même ensemble de symboles.*

En particulier si le coefficient du premier terme de B est le nombre 1, il suffira que la soustraction soit possible dans l'ensemble des symboles où l'on prend les coefficients de A et de B.

Considérons par exemple l'un des cas les plus importants pour la suite : la *division des polynomes par* $x - a$; l'identité à écrire sera

$$A = (x - a).Q + R,$$

et R se réduira à un nombre rationnel. Pour obtenir ce nombre il suffira de remplacer x par un nombre rationnel quelconque; nous choisirons le nombre a, qui a l'avantage de ne pas exiger le calcul de Q. Si en effet on fait $x = a$ dans l'identité précédente le polynome $A(x)$ devient un nombre rationnel déterminé $A(a)$, $Q(x)$ devient également un nombre rationnel $Q(a)$, dont le produit par zéro est zéro, et l'on a par suite

$$A(a) = R.$$

On peut donc dire : *Si un polynome* $A(x)$ *est divisible par* $(x - a)$, $A(a)$ *est égal à zéro et réciproquement.*

On verrait aisément que si l'on a également $A(b) = 0$, le polynome est divisible par $(x - a)(x - b)$, etc., etc... Il résulte de là que si on considère m nombres $a, b, \ldots, l$ pour lesquels on suppose $A(a) = A(b) = \cdots = A(l) = 0$, le polynome $A(x)$, supposé de degré m, pourra s'écrire

$$A(x) = \lambda(x - a)(x - b)\ldots(x - l),$$

λ étant un nombre rationnel déterminé. Il est bien clair que ce polynome $A(x)$ ne devient égal à zéro pour aucun nombre rationnel

différent de a, b, ..., l, puisqu'un produit de nombres rationnels n'est zéro que si l'un de ces nombres est lui-même zéro. On peut donc affirmer qu'*il n'existe pas de polynome en x de degré m qui prenne la valeur zéro pour $m+1$ choix différents du nombre rationnel x.*

Le polynome $A(x)$ sera d'ailleurs complètement déterminé lorsqu'on donnera en outre le nombre rationnel qu'il représente pour un choix de x différent de $a, b, \ldots, l$. Ecrivons par exemple $A(r) = R$; on en déduira $R = \lambda(r-a)(r-b)\ldots(r-l)$, ce qui détermine λ d'une manière unique. *Un polynome de degré m est donc déterminé par ce fait qu'il devient égal à zéro pour m choix différents $a, b, \ldots, l$ du nombre rationnel x et à un nombre rationnel R lorsque $x = r$.*

La proposition précédente va nous amener à une nouvelle propriété des polynomes, qui sera dans la suite d'une grande importance. Nous avons vu qu'un polynome permet de faire correspondre à tout nombre rationnel x un nouveau nombre rationnel ; nous allons établir que la correspondance précédente suffit à définir le polynome et de plus qu'*une telle correspondance est complètement déterminée par $(m+1)$ couples de nombres correspondants qu'on peut prendre arbitrairement.*

Il suffit évidemment pour cela de montrer qu'*il existe un polynome de degré au plus m et un seul qui fait correspondre aux $(m+1)$ nombres $a, b, \ldots, l$ les nombres $\alpha, \beta, \ldots, \lambda$.* Ces couples $a.\alpha$, $b.\beta, \ldots$ sont assujettis à une seule condition qui résulte du fait que le polynome devient pour chaque choix de x un nombre rationnel *bien déterminé*, c'est que si deux des nombres a et b sont égaux, les nombres α et β doivent l'être aussi. Il est bien clair que si cela a lieu, il faut ajouter un nouveau couple, puisque deux des couples donnés coïncident.

La démonstration de la proposition est immédiate : le polynome

$$A(x) = \frac{(x-b)(x-c)\ldots(x-l)}{(a-b)(a-c)\ldots(a-l)}$$

fait correspondre aux nombres $b, c, \ldots, l$ le nombre zéro et au nombre a le nombre 1 ; c'est d'ailleurs le seul polynome possédant cette propriété, d'après un théorème démontré plus haut. Si on définit de même des polynomes $B(x)$, $C(x)$, ..., $L(x)$, le polynome de même degré $\alpha A(x) + \beta B(x) + \ldots + \lambda L(x)$ satisfait aux conditions imposées, c'est-à-dire est de degré au plus égal à m et fait correspondre aux nom-

bres a, b, ..., l les nombres α, β, ..., λ. Il est le seul possédant cette propriété, car s'il en existait un second, la différence de ces deux polynomes serait de degré m et ferait correspondre aux $(m-1)$ nombres a, b, ..., l le même nombre zéro, ce qui a été démontré impossible.

On peut donc dire que la correspondance établie par un polynome entre les nombres rationnels *caractérise* le polynome et de plus qu'elle est complètement donnée par $(m+1)$ couples de nombres correspondants.

Il convient de faire observer ici que le degré du polynome qu'on vient de construire n'est pas nécessairement m, mais peut être inférieur à m. Si par exemple les nombres a et α sont associés de telle sorte que la correspondance puisse être donnée par un polynome de degré inférieur à m, c'est ce polynome que l'on obtiendra d'après la règle précédente. Ainsi le polynome qui fait correspondre aux nombres 1, 2, 3 les nombres 0, 1, 2 est le binome $x-1$; il est aisé d'ailleurs de le vérifier sur la formule

$$0.\frac{(x-2)(x-3)}{(1-2)(1-3)}+1.\frac{(x-3)(x-1)}{(2-3)(2-1)}+2\frac{(x-1)(x-2)}{(3-1)(3-2)}=x-1.$$

La formule $f(x)=\alpha A(x)+\beta B(x)+\ldots\ldots+\lambda L(x)$ qui donne un polynome $f(x)$, de degré au plus égal à m, tel que

$$f(a)=\alpha,\quad f(b)=\beta,\ldots\ldots f(l)=\lambda$$

est connue sous le nom de *formule d'interpolation de Lagrange*.

IV. — Divisibilité des polynomes.

13. Nous allons maintenant exposer rapidement comment on a pu étendre, aux polynomes entiers en x, les notions correspondant à la décomposition des entiers en facteurs. Dans l'étude des entiers positifs on a remarqué que le produit de deux entiers positifs est encore un entier positif, et on a été conduit par là à rechercher si tout entier peut être regardé comme le produit de deux entiers. La réponse négative à cette question a permis de séparer en deux classes les entiers positifs; dans l'une on a mis les nombres qui n'admettent d'autres diviseurs qu'eux-mêmes et l'unité et qu'on a appelés nombres *premiers*, les autres ont été nommés nombres *composés*

On a montré que tout nombre composé peut être mis et d'une seule manière sous forme d'un produit de nombres premiers et on a fondé là-dessus une théorie de la divisibilité des entiers.

Il suffit d'observer que le produit de deux polynomes entiers en x est également un polynome entier en x pour être amené à se poser pour les polynomes la question inverse : tout polynome entier en x peut-il se ramener à un produit de deux polynomes ? Nous avons vu que lorsqu'on a une identité en x : $A = B.Q$, le polynome B est dit *diviseur* de A ; on va montrer qu'étant donné un polynome entier $f(x)$ il est possible de reconnaitre si ce polynome admet des diviseurs et dans ce cas de les trouver par un nombre limité d'opérations.

Supposons le polynome $f(x)$ de degré $2n$ ou $2n+1$; il est clair qu'il suffira de trouver tous les polynomes de degré n au plus qui divisent $f(x)$; s'il existe, en effet, un polynome de degré supérieur à n divisant $f(x)$, il s'obtiendra en divisant $f(x)$ par le produit de polynomes diviseurs de degré inférieur à n.

Soit d'abord un polynome $f(x)$ *à coefficients rationnels ;* nous pouvons multiplier ce polynome par un entier suffisamment grand pour que tous les coefficients deviennent entiers ; si on suppose que chaque coefficient est une fraction irréductible, il suffira de multiplier par le plus petit multiple commun des dénominateurs. On pourra d'ailleurs affirmer qu'après cette opération, les divers coefficients de $f(x)$ *seront sans diviseur commun* et substituer le polynome ainsi obtenu au polynome donné.

Si l'on a, en effet, trouvé

$$A.f(x) = \varphi(x).\psi(x),$$

on en conclut

$$f(x) = \frac{\varphi(x)}{B}\cdot\frac{\psi(x)}{C},$$

sous la seule condition $B.C = A$, A, B, C étant des nombres rationnels quelconques.

Nous conviendrons donc *de rendre le polynome donné $f(x)$ à coefficients entiers sans diviseur commun et de n'appeler* DIVISEURS *de $f(x)$ que les diviseurs du polynome ainsi modifié.*

A l'égard des polynomes entiers en x dont les coefficients sont entiers, Gauss a établi la proposition suivante : *si un polynome à coef-*

ficients entiers est décomposable en un produit de deux polynomes, ces polynomes sont aussi à coefficients entiers.

Remarquons d'abord que si $\varphi(x)$ et $\psi(x)$ sont des polynomes à coefficients entiers, dans chacun desquels le plus grand commun diviseur des coefficients est l'unité, il en est de même du produit $\varphi(x).\psi(x)$. Il suffit, pour le prouver, de montrer que tout nombre premier p qui divise tous les coefficients du produit divise aussi tous les coefficients d'un des facteurs.

Or nous pouvons toujours écrire $\varphi(x)$ et $\psi(x)$ sous la forme

$$\varphi(x) = p\varphi_1(x) + \varphi_2(x),$$

$$\psi(x) = p\psi_1(x) + \psi_2(x),$$

φ_1, φ_2, ψ_1, ψ_2 étant des polynomes à coefficients entiers dont certains peuvent être identiquement nuls et *aucun coefficient de φ_2 ni de ψ_2 n'étant divisible par p.*

Mais on a identiquement

$$[\varphi - p.\varphi_1][\psi - p.\psi_1] = \varphi_2.\psi_2;$$

il en résulte que le second membre de cette identité est divisible par p. Cela est manifestement impossible sans que l'un des polynomes φ_2 et ψ_2 se réduise à zéro. En effet, le terme de plus haut degré du produit $\varphi_2.\psi_2$ n'est certainement pas divisible par p d'après l'hypothèse même faite sur les coefficients de φ_2 et ψ_2. Donc l'un des polynomes φ_2, ψ_2 se réduit à zéro et le polynome φ, ψ correspondant a ses coefficients divisibles par p.

La proposition de Gauss est maintenant immédiate. Soit $f(x)$ un polynome à coefficients entiers qui est le produit de deux polynomes $\varphi(x)$ et $\psi(x)$ à coefficients rationnels ; en multipliant par le plus petit multiple commun des dénominateurs on peut écrire

$$A.f(x) = B.\varphi_1(x).\psi_1(x),$$

A et B étant des entiers, φ_1 et ψ_1 étant des polynomes dont les coefficients sont des entiers sans diviseur commun. Le plus grand diviseur commun aux coefficients du second membre développé est donc B ; il en résulte que A divise B, et si l'on pose

$$B = A.C,$$

on aura

$$f(x) = C.\varphi_1(x).\psi_1(x),$$

ce qui démontre la proposition de Gauss. Le nombre C est d'ailleurs le plus grand diviseur commun aux coefficients de $f(x)$.

14. Nous avons appris ainsi qu'étant donné un polynome $f(x)$ dont les coefficients sont des entiers sans diviseur commun, *il suffit de rechercher les diviseurs de $f(x)$ parmi les polynomes dont les coefficients possèdent la même propriété.*

Soit donc maintenant

$$f(x) = g(x).h(x),$$

g et h étant à coefficients entiers; on aura, quel que soit l'entier a,

$$f(a) = g(a).h(a),$$

ce qui montre que l'entier $g(a)$ est nécessairement diviseur de $f(a)$; il existe donc pour $g(a)$ un nombre limité de valeurs possibles.

Donnons-nous le degré de $g(x)$, pris comme on l'a remarqué plus haut parmi les nombres $1, 2, \ldots, n$; soit p ce degré. Le polynome $g(x)$ sera complètement déterminé si l'on connaît les entiers qu'il fait correspondre à $(p+1)$ entiers quelconques $a, b, \ldots, k$. Les nombres $g(a), g(b), \ldots, g(k)$ sont respectivement des diviseurs positifs ou négatifs des nombres $f(a), f(b), \ldots, f(k)$.

Il suffit donc de combiner les diviseurs de $f(a), f(b), \ldots, f(k)$ entre eux de toutes les manières possibles en prenant un diviseur et un seul de chacun de ces nombres et de former les polynomes de degré p qui pour $a, b, \ldots, l$ deviennent égaux à ces diviseurs. On obtiendra ainsi un nombre limité de polynomes qu'il suffira d'essayer pour trouver, s'il en existe, les diviseurs de degré p de $f(x)$. Il est clair qu'il y aura tout avantage à choisir les nombres $a, b, \ldots, k$ de façon que les entiers $f(a), f(b), \ldots, f(k)$ aient aussi peu de diviseurs que possible. En cherchant successivement les diviseurs du premier degré, puis du second, du troisième, etc., *on sera assuré de ne jamais faire d'opération inutile.* Il faut remarquer qu'un diviseur étant trouvé, il est nécessaire de s'assurer s'il n'est pas diviseur multiple de $f(x)$, c'est-à-dire si le quotient de $f(x)$ par ce diviseur est encore ou non divisible par le même diviseur. Dans le cas où cela se présente, il faut avant de chercher de nouveaux diviseurs débarrasser $f(x)$ complètement de ce diviseur multiple.

Enfin il est inutile de s'occuper des polynomes que l'on obtient par la formule de Lagrange lorsque leurs coefficients ne sont pas entiers.

Soit par exemple à étudier le polynome $x^3 + x^2 - x + 2$ au point de vue de sa décomposition en facteurs. Il suffit de chercher ses diviseurs du premier degré. Nous avons, en prenant pour nombres $a, b, \ldots, k$ les nombres 0 et 1,

$$f(0) = 2,$$
$$f(1) = 3,$$

ce qui donne pour $g(0)$ et $g(1)$ les systèmes

$$\begin{cases} g(0) = \pm 1, \pm 2\,; \\ g(1) = \pm 1, \pm 3. \end{cases}$$

On peut évidemment se borner à considérer les diviseurs, *abstraction faite de leur signe*, c'est-à-dire seulement les huit combinaisons

$g(0)$	$g(1)$	$g(0)$	$g(1)$
1	1	2	1
1	—1	2	—1
1	3	2	3
1	—3	2	—3

D'ailleurs comme on a ici $A(x) = 1 - x$ et $B(x) = x$, les binomes obtenus sont respectivement

$$1 - x + x, \quad 1 - x - x, \quad 1 - x + 3x, \quad 1 - x - 3x$$

et

$$2 - 2x + x, \quad 2 - 2x - x, \quad 2 - 2x + 3x, \quad 2 - 2x - 3x.$$

Parmi ces binomes on peut écarter *a priori* ceux qui ne renferment pas x et ceux pour lesquels le coefficient de x est autre que ± 1, car il résulte des règles de la multiplication des polynomes que le coefficient de x^3 dans $f(x)$ doit être divisible par celui de x dans $g(x)$.

Il reste donc à essayer seulement les deux binomes $2 - x$ et $2 + x$, et l'on voit aisément que $2 + x$ convient seul. En effectuant la division on a donc

$$x^3 + x^2 - x + 2 = (x + 2).(x^2 - x + 1),$$

et la décomposition est terminée puisque $x + 2$ ne divise pas $x^2 - x + 1$.

Ajoutons que la méthode précédente est loin d'être la plus simple *lorsqu'on se borne à rechercher les diviseurs du premier degré du*

polynome $f(x)$. Habituellement on opère de la manière suivante : Si l'un des diviseurs est $qx - p$, on aura $f\left(\frac{p}{q}\right) = 0$, c'est-à-dire

$$ap^m + bp^{m-1}q + \dots + lq^n = 0,$$

d'où il résulte que p divise l et q divise a, en supposant bien entendu p et q sans diviseur commun.

Il suffit par conséquent d'essayer les binomes $qx - p$, où q est un diviseur de x et p un diviseur de l.

Nous venons d'établir que *par un nombre limité d'opérations* il est possible de trouver tous les polynomes de degré donné p qui divisent un polynome $f(x)$; lorsqu'on a procédé méthodiquement en cherchant d'abord les diviseurs du premier degré, puis ceux du second, etc., on peut affirmer que les polynomes trouvés n'admettent aucun diviseur. En effet, un diviseur du second degré, par exemple, ne pourrait admettre qu'un diviseur du premier degré et on les a tous obtenus et supprimés dans $f(x)$ lorsqu'on cherche les diviseurs du second degré.

On peut donc écrire une décomposition de $f(x)$ absolument analogue à la décomposition d'un nombre entier en facteurs premiers

$$f = g^\alpha . h^\beta \dots l^\lambda.$$

Les polynomes $g, h, \dots l$, qui n'admettent aucun diviseur, sont dits *irréductibles*; ils jouent manifestement le rôle que jouent les nombres premiers en Arithmétique.

Il est facile de voir qu'il existe des polynomes irréductibles de degré quelconque, le binome $x^n + 2$ où n est quelconque en est évidemment un; il en est de même de $x^{p-1} + x^{p-2} + \dots + x + 1$ lorsque p est un nombre premier; nous le démontrerons plus loin.

15. Tout polynome entier en x, à coefficients entiers sans diviseur commun, est irréductible ou décomposable en un produit de polynomes irréductibles dont les coefficients possèdent la même propriété. Il reste à prouver qu'*une telle décomposition n'est possible que d'une seule manière*, et pour cela nous sommes obligés de faire appel à l'algorithme du plus grand commun diviseur étendu aux polynomes. L'existence de l'algorithme d'Euclide pour les polynomes est une simple conséquence de l'existence de l'identité de la division $A = B.Q + R$.

Supposons A et B à coefficients entiers, ce qu'il est toujours permis de faire ; on peut remarquer d'abord qu'il suffit de multiplier A par un entier convenable, le coefficient du premier terme de B élevé à une certaine puissance, pour n'introduire dans Q et dans R que des nombres entiers.

Si l'on écrit alors $\alpha A = B.Q + R$, on peut en conclure que les diviseurs communs à A et à B sont les mêmes que les diviseurs communs à B et à R. En continuant à déterminer les polynomes R_1, R_2, ... qui vérifient les identités

$$\alpha_1 B = R.Q_1 + R_1,$$
$$\alpha_2 R = R_1.Q_2 + R_2,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\ldots\ldots\ldots\ldots\ldots\ldots,$$

dans lesquelles α_i est une puissance du coefficient du premier terme de R_{i-1}, on parvient soit à un reste R_n nul, soit à un reste R_n qui est un nombre entier autre que zéro.

Dans le premier cas les diviseurs communs à A et à B sont les mêmes que les diviseurs de R_{n-1}, on dit que R_{n-1} *est le plus grand commun diviseur* des polynomes A et B ; dans le second cas, A et B n'ont aucun diviseur commun, on dit qu'ils sont *premiers entre eux*.

La suite des identités qu'on vient d'écrire devient manifestement, lorsqu'on remplace A et B par A.M et B.M, M étant un polynome quelconque à coefficients entiers :

$$\alpha_1 B.M = R.M.Q_1 + R_1.M,$$
$$\alpha_2 R.M = R_1.M.Q_1 + R_2.M,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\ldots\ldots\ldots\ldots\ldots\ldots;$$

d'où il résulte que : 1° Si A et B ont pour plus grand commun diviseur D, AM et BM ont pour plus grand commun diviseur DM ;

2° Si A et B sont premiers entre eux, A.M et B.M ont pour plus grand commun diviseur M.

Cela va nous permettre de démontrer la proposition suivante, qui est fondamentale dans cette théorie : *Un polynome irréductible* C *qui divise le produit* A.B *de deux polynomes* A *et* B *divise nécessairement l'un d'eux.*

Supposons en effet que C ne divise pas A, il sera premier avec A puisqu'ils ne peuvent avoir de diviseur commun autre que C; le plus grand commun diviseur à C.B et à A.B sera par conséquent B. Il suit de là que C, qui divise C.B et A.B, est un diviseur de leur plus grand commun diviseur B. C'est ce qu'il fallait démontrer.

On déduit immédiatement de ce théorème que lorsqu'un polynome irréductible divise un produit de polynomes irréductibles, il est identique à l'un d'eux. D'une manière générale pour que le polynome $f(x)$ soit un diviseur de $F(x)$, il faut et il suffit que $f(x)$ ne renferme que des facteurs irréductibles de $F(x)$ affectés d'un exposant au plus égal à celui qu'ils ont dans $F(x)$.

Si l'on avait par conséquent deux décompositions de $f(x)$ en facteurs irréductibles, chacune d'elles devrait diviser l'autre et par suite elles renfermeraient les mêmes facteurs à la même puissance, c'est-à-dire seraient identiques. On peut donc affirmer que la décomposition d'un polynome en facteurs irréductibles n'est possible que d'une seule manière. Nous avons donné le moyen de trouver une décomposition, il est par conséquent inutile d'en chercher d'autres.

V. — Polynomes à plusieurs variables.

16. Les propositions précédentes sur les polynomes à une variable x s'étendent naturellement aux polynomes à plusieurs variables $x_1, x_2, \ldots, x_n$, c'est-à-dire aux expressions qui sont la somme d'un nombre limité de termes :

$$A.x_1^{\alpha}.x_2^{\beta}.\ldots.x_n^{\lambda},$$

A désignant un nombre rationnel, $\alpha, \beta, \ldots, \lambda$ des entiers positifs et $x_1, x_2, \ldots, x_n$, des nombres rationnels indéterminés. C'est toujours dans ce sens de symboles *connus* dont on ne fixe pas la détermination, que nous emploierons le mot *variables*.

On peut évidemment, comme pour les polynomes à une variable x, se borner ici à l'étude des polynomes à coefficients entiers. Nous allons seulement mettre en évidence la possibilité d'une décomposition, par un nombre fini d'essais, d'un polynome à n variables $x_1, \ldots, x_n$ en un produit de polynomes irréductibles.

Le problème qui consiste à trouver les diviseurs de $f(x_1, x_2, \ldots, x_n)$ se ramène par un artifice ingénieux dû à Kronecker, au problème analogue, déjà résolu, pour les polynomes à une seule variable.

Désignons par g un entier positif qui surpasse l'exposant le plus élevé de chacune des variables $x_1, x_2, \ldots, x_n$ dans $f(x_1, \ldots, x_n)$. Il est clair que si $f(x_1, \ldots, x_n)$ est décomposable en facteurs, g dépassera aussi le plus grand des exposants de $x_1, \ldots, x_n$ dans chacun de ces facteurs.

Posons alors

$$x_1 = x, \quad x_2 = x^g, \quad x_3 = x^{g^2}, \ldots \quad x_n = x^{g^{n-1}},$$

en désignant par x une nouvelle indéterminée, *ce qui revient à considérer le cas où les nombres rationnels $x_1, x_2, \ldots, x_n$ au lieu d'être absolument arbitraires sont toujours des fonctions déterminées de l'un d'entre eux*. On voit aisément que si $f(x_1, \ldots, x_n)$ est décomposable lorsque $x_1, \ldots, x_n$ ne sont pas liés entre eux, il en sera de même du polynome $F(x)$ que l'on fait ainsi correspondre à f.

A tout monome tel que $Ax_1^{\alpha_1} \ldots x_n^{\alpha_n}$ correspond dans le polynome $F(x)$ le monome $Ax^{\alpha_1 + \alpha_2 g + \alpha_3 g^2 + \cdots + \alpha_n g^{n-1}}$, dans lequel on peut considérer l'exposant de x comme le nombre

$$\alpha_n \alpha_{n-1} \ldots \alpha_2 \alpha_1$$

supposé écrit dans le système de numération de base g. Cela résulte de l'hypothèse que les exposants $\alpha_n, \ldots, \alpha_1$ sont tous inférieurs à g.

D'ailleurs la correspondance ainsi établie est univoque, c'est-à-dire qu'aux termes différents de $f(x_1, \ldots, x_n)$ correspondent dans $F(x)$ des termes de degrés différents. *Il n'y a donc, après la transformation, aucune réduction possible des termes de* $F(x)$ *entre eux*.

Nous savons qu'à toute égalité

$$f(x_1, \ldots, x_n) = g(x_1, \ldots, x_n) \cdot h(x_1, \ldots, x_n)$$

correspond une égalité

$$F(x) = G(x) \cdot H(x),$$

G et H désignant les transformées respectives de g et h. Il suffit donc pour savoir si f admet ou non des diviseurs, de chercher les diviseurs irréductibles $G(x)$ de $F(x)$, d'écrire pour chacun d'eux l'identité en x

$$F(x) = G(x) \cdot H(x)$$

et de transformer cette identité par la substitution inverse, ce qui

donne

$$f(x_1, x_2, \ldots, x_n) = g(x_1, x_2, \ldots, x_n).h(x_1, \ldots, x_n).$$

Si l'on obtient ainsi une identité en $x_1, x_2, \ldots, x_n$, on peut affirmer que $g(x_1, \ldots, x_n)$ est bien un diviseur irréductible de $f(x_1, \ldots, x_n)$. Si $h(x_1, \ldots, x_n)$ n'est pas divisible par $g(x_1, \ldots, x_n)$, on opérera sur $h(x_1, \ldots, x_n)$ comme on a opéré sur $f(x_1, \ldots, x_n)$; on parviendra ainsi par un nombre limité d'essais à la décomposition de $f(x_1, \ldots, x_n)$ en facteurs irréductibles où l'on reconnaitra l'absence de toute décomposition.

Supposons que dans un polynome à plusieurs variables $x_1, x_2, \ldots, x_n$ on porte spécialement l'attention sur l'une d'elles x_1, qu'on appellera x, les autres étant considérées comme des nombres rationnels indéterminés $a, b, \ldots, l$. Nous pouvons toujours supposer que dans le polynome $f(x, a, b, \ldots, l)$ les coefficients des diverses puissances de x sont des polynomes en $a, b, \ldots, l$ sans diviseur commun et à coefficients entiers. S'il n'existe alors aucune identité de la forme

$$f(x, a, b, \ldots, l) = g(x, a, b, \ldots, l).h(x, a, b, \ldots, l)$$

dans laquelle g et h sont des polynomes en $x, a, b, \ldots, l$, on dira que *le polynome en* x $f(x, a, b, \ldots, l)$ est irréductible dans le *domaine d'intégrité* $[a, b, \ldots, l]$ (*).

Il est aisé de voir que les propositions établies sur l'existence des polynomes irréductibles à une variable x, la décomposition unique d'un polynome en facteurs irréductibles, etc.... s'étendent aux polynomes à plusieurs variables et par suite aux polynomes en $x, a, b, \ldots, l$ dont on vient de parler ; nous n'y insisterons pas davantage.

Terminons en observant qu'on peut, en suivant la marche indiquée dans le cas d'une seule variable, introduire des symboles X

(*) On désigne sous le nom de domaine d'intégrité $[a, b, \ldots, l]$ *l'ensemble des polynomes entiers à coefficients entiers des lettres* $a, b, \ldots, l$; un polynome est par conséquent irréductible dans un domaine d'intégrité lorsqu'il n'est pas le produit de deux polynomes dont les coefficients appartiennent à ce domaine.

Cette définition de l'irréductibilité concorde manifestement avec la définition donnée pour un polynome à une variable ; dans cette dernière le domaine d'intégrité est remplacé par l'ensemble des nombres entiers.

définis par des relations de la forme

$$f(x_1, x_2, \ldots, x_n).X = g(x_1, x_2, \ldots, x_n),$$

dans laquelle f et g sont des polynomes et qu'on appelle *fractions rationnelles* des variables $x_1, x_2, \ldots, x_n$. On les représente par le signe $\frac{g(x_1, x_2, \ldots, x_n)}{f(x_1, x_2, \ldots, x_n)}$ et il est bien clair que leurs propriétés sont analogues à celles des fractions ordinaires et s'établissent de même lorsqu'on suppose qu'ils possèdent avec les polynomes deux modes de composition : addition et multiplication, suivant les mêmes lois que les modes correspondants pour les entiers positifs.

CHAPITRE II

LES NOMBRES ALGÉBRIQUES

I. — Définition.

17. Considérons un polynome entier en x à coefficients rationnels,

$$f(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_n;$$

nous savons qu'à tout nombre rationnel x_0, le polynome fait correspondre un nombre rationnel bien déterminé $f(x_0)$.

Nous avons déjà fait observer que le nombre $f(x_0)$ ainsi obtenu n'est pas un nombre rationnel quelconque, c'est-à-dire qu'étant donné un nombre rationnel y_0 il n'existe pas nécessairement de nombre rationnel x_0 tel que l'on ait l'égalité

$$y_0 = f(x_0).$$

Il est aisé de reconnaître, lorsqu'on donne le nombre y_0, si une telle égalité peut avoir lieu. Considérons à cet effet le polynome entier $f(x) - y_0$; s'il existe un nombre rationnel x_0 qui vérifie l'égalité $f(x_0) = y_0$, ce nombre annule le polynome $f(x) - y_0$, et réciproquement. On est donc amené à rechercher les nombres rationnels qui, mis à la place de x, annulent le polynome $f(x) - y_0$.

Remarquons immédiatement qu'il suffira de considérer au lieu de $f(x) - y_0$, tout polynome à coefficients entiers qu'on peut en déduire en multipliant cette expression par un entier convenable et, en particulier, celui de ces polynomes dont tous les coefficients sont des entiers sans diviseur commun.

Soit donc $F(x)$ un polynome entier satisfaisant à cette condition; si $\frac{b}{a}$ est un nombre rationnel tel que l'on ait $F\left(\frac{b}{a}\right) = 0$, le

polynome $F(x)$ est divisible par $ax - b$; inversement, si l'on a

$$F(x) = (ax - b) G(x),$$

le polynome $F(x)$ s'annule pour $x = \frac{b}{a}$. On conclut de là que *tout polynome entier qui admet des diviseurs du premier degré, peut représenter le nombre zéro pour des déterminations rationnelles de la variable*. Il existe autant de représentations qu'il existe de diviseurs du premier degré différents.

Si, au contraire, un polynome entier n'admet pas de diviseurs du premier degré, il n'existe pas de nombre rationnel qui annule le polynome.

Cette remarque nous amène à étendre de nouveau l'ensemble des symboles sur lesquels nous raisonnons, et nous allons le faire en suivant absolument la méthode employée pour l'introduction des nombres rationnels.

18. Considérons un polynome entier en x à coefficients rationnels, $f(x)$, *irréductible* au sens que nous avons adopté plus haut. Il n'existe aucun nombre rationnel qui, mis à la place de x, vérifie la relation $f(x) = 0$ lorsque, comme nous le supposons naturellement, le degré n de $f(x)$ est différent de l'unité.

Nous allons ajouter à l'ensemble des nombres rationnels des symboles nouveaux qui, *par définition*, vérifieront cette relation. Il est évidemment nécessaire, pour que cela ait un sens, que nous ayons défini pour ces symboles des opérations que nous appellerons addition et multiplication et qui conduisent d'une manière unique et déterminée au polynome $f(x)$ lorsqu'on donne x. Il nous faut donc définir deux modes de composition de ces symboles entre eux et avec les nombres rationnels ; *nous pouvons d'ailleurs, au point de vue logique, faire cela d'une manière arbitraire*. Nous nous attacherons, pour la simplicité des résultats, à conserver à ces deux modes de composition les propriétés fondamentales de l'addition et de la multiplication qu'on a trouvées pour les nombres entiers.

Ainsi l'ensemble des nouveaux symboles et des anciens sera tel que :

1° De deux d'entre eux on puisse déduire un troisième d'une manière unique, la composition ainsi définie possédant les quatre propriétés fondamentales de l'addition ;

2° De deux d'entre eux, par un second mode de composition, on puisse déduire un troisième symbole, la composition possédant les cinq propriétés fondamentales de la multiplication.

Enfin on conservera la manière d'écrire employée pour l'addition et la multiplication des entiers.

Avant d'aller plus loin, nous pouvons remarquer que la propriété distributive de la multiplication permet d'écrire

$$x.(y+0) = x.y + x.0,$$

x et y étant deux quelconques de nos symboles ; et comme l'on a $y+0=y$, il en résulte $x.0=0$; donc *le produit d'un quelconque des nouveaux symboles par zéro sera zéro*. La propriété commutative de la multiplication montre qu'on a également $0.x=0$.

Si maintenant nous considérons les produits $x.0$ et $x.y$, en supposant x différent de zéro, on peut conclure de la cinquième propriété fondamentale de la multiplication que lorsque y est différent de zéro, le produit $x.y$ n'est pas zéro. Il résulte de là qu'*un produit de deux symboles n'est nul que si l'un des symboles est nul*. C'est là une importante proposition dont nous aurons bientôt à nous servir.

19. Jusqu'à présent nous n'avons pas défini les symboles que nous voulons introduire, nous n'avons défini que leurs modes de composition. Ce que nous avons dit prouve qu'il sera possible, lorsque les symboles seront définis, de définir d'une manière précise ce que c'est qu'un polynome ou une fraction rationnelle dont les éléments : coefficients ou variables, sont ces nouveaux symboles.

Désignons maintenant par x_1 un symbole satisfaisant aux conditions précédentes et vérifiant la relation $f(x_1)=0$. Nous pouvons conclure de là que $f(x)$ est divisible par $(x-x_1)$, c'est-à-dire qu'il existe une identité en x telle que :

$$f(x) = (x-x_1)f_1(x, x_1),$$

$f_1(x, x_1)$ étant un polynome entier en x de degré $n-1$ dont les coefficients sont des polynomes entiers en x_1. En effet, la théorie de la divisibilité d'un polynome par $x-a$ repose sur l'existence d'une identité,

$$A = BQ + R,$$

lorsque A est un polynome de degré supérieur à B. Cette identité

peut être écrite ici, d'après les hypothèses faites sur x_1, et donnera

$$f(x) = (x - x_1)f_1(x, x_1) + f(x_1);$$

comme nous supposons par définition $f(x_1) = 0$, il en résulte

$$f(x) = (x - x_1)f_1(x, x_1).$$

Lorsqu'on a introduit, dans le calcul, les nombres rationnels par une relation

$$a.x - 1 = 0,$$

les propriétés fondamentales de la multiplication ont permis d'établir l'existence d'un seul symbole possédant les modes de composition indiqués et tel que $a.x - 1 = 0$. Il n'en est plus de même ici; nous allons voir, en effet, qu'*il existe n symboles possédant les modes de composition ci-dessus désignés et vérifiant la relation* $f(x) = 0$, de sorte qu'on est conduit à ajouter simultanément ces n symboles à l'ensemble des nombres rationnels.

Soit, en effet, x_2 un symbole tel que l'on ait $f(x_2) = 0$; l'identité en x

$$f(x) = (x - x_1)f_1(x, x_1)$$

donnera

$$f(x_2) = (x_2 - x_1) f_1(x_2, x_1);$$

on voit qu'il n'en résulte pas nécessairement $x_2 - x_1 = 0$; si l'on suppose, par conséquent, x_2 différent de x_1, on aura

$$f_1(x_2, x_1) = 0.$$

Le symbole x_2 annule donc le polynome $f_1(x, x_1)$, autrement dit de l'identité en x

$$f_1(x, x_1) = (x - x_2)f_2(x, x_1, x_2) + f_1(x_2, x_1),$$

que l'on peut toujours écrire, d'après les hypothèses faites sur x_1 et x_2, et où f_2 est un polynome entier en x de degré $(n-2)$, à coefficients entiers en x_1 et x_2, on peut déduire

$$f_1(x, x_1) = (x - x_2)f_2(x, x_1, x_2),$$

x_1 et x_2 ayant la signification supposée.

En continuant ainsi, on mettra $f(x)$ sous la forme

$$f(x) = (x - x_1)(x - x_2)\ldots(x - x_n),$$

$x_1, x_2, \ldots, x_n$ étant des symboles différents, c'est-à-dire que dans le calcul on devra regarder les différences $x_i - x_k$ comme différentes de zéro.

Nous supposons bien entendu que le coefficient de x^n dans $f(x)$ a été ramené à être l'unité, sans quoi il aurait fallu introduire dans le second membre un facteur égal à ce coefficient.

Je dis qu'*il n'existe plus d'autre symbole x_p possédant les propriétés indiquées et tel que l'on ait $f(x_p)=0$*. On déduirait en effet de cette relation

$$(x_p - x_1)(x_p - x_2)\dots(x_p - x_n) = 0,$$

et comme le produit d'un certain nombre de nos symboles n'est nul que si l'un d'eux est égal à zéro, il en résulte que x_p est l'un des symboles déjà introduits.

Nous sommes donc amenés à considérer *simultanément* n symboles $x_1, x_2, \dots, x_n$ possédant les propriétés indiquées et vérifiant la relation $f(x) = 0$ ou les équations successives

$$f(x_1) = 0, \qquad \frac{f(x_2) - f(x_1)}{x_2 - x_1} = f_1(x_2, x_1) = 0,$$

$$\frac{f_1(x_3, x_1) - f_1(x_2, x_1)}{x_3 - x_2} = f_2(x_3, x_2, x_1) = 0, \quad \text{etc.}\ .$$

Ajoutons qu'on peut encore regarder $x_1, x_2, \dots, x_n$ comme définis par l'identité en x

$$f(x) = (x - x_1)(x - x_2)\dots(x - x_n);$$

si nous posons, par exemple,

$$f(x) = x^n - p_1x^{n-1} + p_2x^{n-2} \cdots \pm p_n,$$

l'identification donnera entre les symboles $x_1, x_2, \dots, x_n$ les relations

$$x_1 + x_2 + \cdots + x_n = p_1,$$
$$x_1x_2 + \cdots + x_{n-1}x_n = p_2,$$
$$\dots\dots\dots\dots$$
$$\dots\dots\dots\dots$$
$$x_1x_2 \dots\dots\dots x_n = p_n.$$

Ces relations sont équivalentes aux relations

$$f(x_1) = 0, \qquad f_1(x_2, x_1) = 0, \qquad f_2(x_3, x_2, x_1) = 0, \quad \text{etc.}\dots,$$

c'est-à-dire que les unes sont des conséquences nécessaires des autres et réciproquement. Il serait aisé de le vérifier; nous y reviendrons plus loin.

Nous avons maintenant à développer les conséquences logiques des hypothèses faites sur les symboles $x_1, x_2, \ldots, x_n$, c'est-à-dire à constituer le calcul de ces symboles tel qu'il résulte de ces hypothèses. Il résultera clairement de ce calcul que les hypothèses qu'on a faites sur $x_1, x_2, \ldots, x_n$ ne sont pas contradictoires, c'est-à-dire qu'il est effectivement possible de définir logiquement des symboles $x_1, x_2, \ldots x_n$ *autres que les nombres rationnels,* possédant avec ces derniers deux modes de composition : addition et multiplication, qui suivent les mêmes lois que ces modes dans le calcul des entiers, et qui vérifient en outre les relations

$$f(x_1) = 0, \qquad f_1(x_2, x_1) = 0, \quad \ldots.$$

écrites plus haut.

Mais, alors que le développement des hypothèses faites sur les symboles qu'on a appelés « entiers négatifs » et « nombres rationnels » résulte immédiatement des propriétés bien connues des nombres entiers positifs, celui des hypothèses faites sur $x_1, x_2, \ldots, x_n$ exige une étude plus approfondie des propriétés des polynomes à une et à plusieurs variables. Cette étude constituera le chapitre suivant et ce n'est que dans un chapitre ultérieur que l'on montrera d'une part, qu'il est possible de déduire toutes les conséquences nécessaires des relations qui servent à définir $x_1, x_2, \ldots, x_n$ d'un nombre limité d'entre elles, n'impliquant manifestement pas de contradiction, et, d'autre part, qu'*à des questions de notation près*, provenant de ce qu'on n'a pu désigner les symboles qui annulent $f(x)$ par $x_1, x_2, \ldots, x_n$ que dans un ordre arbitraire, le calcul de ces symboles est complètement déterminé et *connu* d'après les hypothèses faites. D'une manière plus précise, on saura décider si deux fonctions bien définies de $x_1, x_2, \ldots, x_n$ sont égales et on pourra donner leur somme et leur produit. Nous aurons, évidemment, répondu ainsi à toutes les objections.

20. Nous commencerons néanmoins par faire ici, au sujet du calcul des symboles $x_1, x_2, \ldots, x_n$, quelques observations générales dont il sera tiré parti plus loin.

Bornons-nous d'abord au calcul du symbole x_1 et des symboles dérivés de sa composition avec lui-même et avec les nombres rationnels. Parmi ces symboles, ceux qui renferment seulement des puissances positives entières de x_1 se ramènent immédiatement à

l'aide de la relation $f(x_1) = 0$, à la forme

$$a + bx_1 + cx_1^2 + \dots + lx_1^{n-1},$$

où $a, b, \dots, l$ sont des nombres rationnels quelconques.

Tous ces symboles sont définis d'une manière unique, et l'hypothèse faite sur la composition par addition ou multiplication du symbole x_1 et des nombres rationnels permet d'étendre, au calcul de ces symboles, les lois du calcul des polynomes, c'est-à-dire celles du calcul des entiers positifs.

Nous allons montrer que toutes les *relations rationnelles* que vérifie x_1 sont des conséquences nécessaires de $f(x_1) = 0$.

Supposons, en effet, que l'on ait $\varphi(x_1) = 0$, φ désignant *un polynome* qu'on peut supposer à coefficients entiers; les opérations qui conduisent au plus grand commun diviseur entre $f(x)$ et $\varphi(x)$ donneront certainement un résultat. Sinon, en effet, on parviendrait à une identité de la forme

$$F(x).\varphi(x) + \Phi(x).f(x) = a,$$

a étant un entier autre que zéro, et lorsqu'on y fait $x = x_1$, cette identité conduit à une contradiction. Mais $f(x)$ est irréductible par hypothèse; il en résulte que $\varphi(x)$ est au moins de degré n et admet $f(x)$ comme diviseur.

La relation $\varphi(x_1) = 0$ est donc une conséquence de $f(x_1) = 0$; en d'autres termes : *Tout polynome $\varphi(x)$, qui s'annule pour l'un des symboles qui annulent le polynome irréductible $f(x)$, est divisible par $f(x)$.*

On peut conclure de là que *tous les polynomes entiers en x_1 de degré inférieur à n sont nécessairement différents*, car une égalité entre deux de ces polynomes donnerait précisément, si elle n'est pas une identité, un polynome entier s'annulant pour $x = x_1$.

Nous allons continuer en étudiant les fractions rationnelles en x_1 à coefficients rationnels, c'est-à-dire les expressions de la forme $\frac{P(x_1)}{Q(x_1)}$, où P et Q sont deux polynomes entiers de degré inférieur à n. Tout d'abord on peut affirmer que $Q(x)$ et le polynome *irréductible* $f(x)$ n'ont aucun diviseur commun; l'algorithme du plus grand commun diviseur conduit donc à une identité en x :

$$q(x).f(x) + Q(x).F(x) = 1,$$

où $q(x)$ et $F(x)$ sont des polynomes entiers. On déduit de là, en multipliant les deux membres par $\frac{P(x)}{Q(x)}$,

$$\frac{P(x).q(x)}{Q(x)} \cdot f(x) + P(x).F(x) = \frac{P(x)}{Q(x)},$$

ce qui montre que, pour tout symbole x_1 qui annule $f(x)$, on a

$$\frac{P(x_1)}{Q(x_1)} = P(x_1).F(x_1)$$

ou, en développant le second membre et le réduisant à l'aide de la relation $f(x_1) = 0$,

$$\frac{P(x_1)}{Q(x_1)} = R(x_1),$$

R étant un polynome entier de degré inférieur à n. *On n'introduit donc pas, par la considération des fractions rationnelles de x_1, d'autres symboles que ceux que l'on a déjà considérés.* On peut donc conclure définitivement que *le calcul de x_1 seul se réduit à celui des polynomes entiers en x_1 de degré inférieur à n, en y négligeant simplement les multiples de $f(x_1)$.*

La relation $f(x) = (x - x_1)(x - x_2)\ldots(x - x_n)$, symétrique en $x_1, x_2, \ldots, x_n$, permettrait d'appliquer le même raisonnement à tous les symboles $x_1, x_2, \ldots, x_n$, et par conséquent de ne considérer que les polynomes entiers en $x_1, x_2, \ldots x_n$ de degré inférieur à n par rapport à chacune de ces lettres; mais nous allons voir que la considération du système de relations donnant les liaisons entre $x_1, x_2, \ldots, x_n$ permet encore de restreindre le nombre des symboles à introduire.

Cela apparaîtra immédiatement si l'on considère le système de relations

$$f(x_1) = 0, \qquad f_1(x_2, x_1) = 0, \qquad f_2(x_3, x_2, x_1) = 0, \quad \text{etc}\ldots$$

On voit, en effet, qu'à l'aide de $f(x_1) = 0$ toute fonction rationnelle de x_1 se réduit à un polynome entier de degré inférieur à n; à l'aide de $f_1(x_2, x_1) = 0$ et de $f(x_1) = 0$ toute fonction rationnelle de x_1 et x_2 se réduit à un polynome entier en x_1 et x_2 de degré inférieur à n en x_1 et inférieur à $(n-1)$ en x_2, etc., etc.

En résumé, *les symboles à introduire sont compris parmi les fonctions entières de $x_1, x_2, \ldots, x_n$ à coefficients rationnels et de degré inférieur à $(n - i + 1)$ par rapport au symbole x_i.*

21. Pour revenir à un autre ordre d'idées, l'introduction des symboles qui, soumis aux conditions déjà données, vérifient $f(x) = 0$ revient à l'adjonction aux groupes formés par les nombres rationnels pour les deux modes de composition : addition et multiplication, *de n nouveaux symboles* $x_1, x_2, \ldots, x_n$ *et de n relations fondamentales* entre ces symboles et les anciens.

Ces relations fondamentales peuvent être écrites sous la forme symétrique

$$\begin{aligned} x_1 + x_2 + \cdots + x_n &= p_1, \\ x_1x_2 + \cdots + x_{n-1}x_n &= p_2, \\ \cdots\cdots\cdots\cdots \\ \cdots\cdots\cdots\cdots \\ x_1x_2 \ldots\ldots\ldots\ldots x_n &= p_n, \end{aligned}$$

ou sous la forme non symétrique

$$f(x_1) = 0, \qquad f_1(x_2, x_1) = 0, \qquad f_2(x_3, x_2, x_1) = 0, \quad \text{etc.}\ldots$$

Nous avons à chercher *si* et *comment*, en tenant compte de ces relations fondamentales et des lois de l'addition et de la multiplication, on peut compléter la *table de structure des groupes* formés de l'ensemble des nombres rationnels et des fonctions rationnelles à coefficients rationnels de $x_1, x_2, \ldots, x_n$, tant au point de vue de l'addition que de la multiplication de leurs éléments.

Il sera donc nécessaire de rechercher d'abord quelles sont parmi ces fonctions celles qui doivent être regardées comme des éléments distincts, et l'on peut affirmer, une fois cela fait, que la table de structure pourra être construite ; — il résultera d'ailleurs de cette table elle-même que les hypothèses faites sur $x_1, \ldots, x_n$ n'entraînent point de contradiction. Le nouvel ensemble pourra donc être regardé comme *connu* vis-à-vis des deux modes de composition : addition et multiplication.

On pourrait *alors* donner des noms à tous les symboles différents ainsi introduits et les représenter par des signes spéciaux, comme on l'a fait pour les entiers négatifs et les nombres rationnels; mais il est préférable, à cause de la complexité des notations qu'il faudrait employer, de les conserver sous la forme, à laquelle on les a réduits, de polynomes entiers en $x_1, x_2, \ldots, x_n$. Cela est d'ailleurs indispensable en ce moment.

Tout ceci étant acquis, on peut imaginer que l'on répète sur

chaque polynome irréductible à coefficients rationnels, dont le premier coefficient est l'unité, ce qu'on vient de faire pour le polynome $f(x)$. On associera par conséquent à tout polynome irréductible $g(y)$, de degré p, des symboles distincts $y_1, y_2, \ldots, y_p$, en nombre p, desquels on suppose qu'ils vérifient l'identité

$$g(y) = (y-y_1)(y-y_2)\cdots(y-y_p)$$

et qu'ils se composent entre eux et avec les nombres rationnels suivant les modes additif et multiplicatif, en suivant les mêmes lois que ces derniers.

Les symboles $x_1, x_2, \ldots, x_n, y_1, \ldots, y_p$ etc... définis de cette manière sont appelés des *nombres algébriques*. Nous observerons d'abord que ces symboles sont tous *distincts*, car deux polynomes irréductibles $f(x)$ et $g(x)$ étant nécessairement premiers entre eux, vérifient une identité de la forme

$$A(x).f(x) + B(x).g(x) = 1$$

et ne peuvent par conséquent s'annuler pour une même détermination de x, qui satisfasse aux conditions imposées à nos symboles. Il est clair qu'il n'en est pas de même des symboles introduits en même temps qu'eux, qui sont leurs fonctions entières à coefficients rationnels ; la relation $x_1 + x_2 + \ldots + x_n = p_1$ écrite plus haut montre par exemple que les symboles $x_1 + \ldots + x_{n-1}$ et $p_1 - x_n$ sont identiques. Elle montre aussi que lorsqu'on a introduit dans le calcul $x_1, x_2, \ldots$ et x_{n-1}, le symbole x_n est déjà *connu* puisqu'il est identique à : $p_1 - x_1 - x_2 \ldots - x_{n-1}$. On est amené ainsi à rechercher les symboles distincts qui figurent dans les polynomes entiers en $x_1, \ldots, x_n$ ou en $y_1, \ldots, y_p$, etc..., et il est aisé de voir qu'il peut arriver que des symboles identiques figurent dans les divers systèmes d'expressions ainsi obtenus. Il sera donc nécessaire de rechercher également quels sont les polynomes entiers en $y_1, \ldots, y_p$ qui sont identiques à des polynomes entiers en $x_1, \ldots, x_n$, pour tous les choix possibles des polynomes irréductibles $f(x)$ et $g(y)$. C'est ce qu'on appellera l'étude simultanée des deux polynomes $f(x)$ et $g(y)$.

Enfin en particulier, on observe qu'il peut se faire que l'un des symboles $y_1, \ldots, y_p$ soit identique à l'un des polynomes entiers en $x_1, \ldots, x_n$ qui sont définis lorsqu'on a défini $x_1, \ldots, x_n$; il sera dans ce cas inutile d'introduire de nouveau ce symbole y_i dans

le calcul. On est conduit par là à *rechercher, parmi tous les nombres algébriques, ceux qu'il est nécessaire et suffisant d'introduire dans le calcul, c'est-à-dire de représenter par des signes explicites, pour pouvoir exprimer rationnellement tous les autres*, c'est-à-dire afin que chaque polynome irréductible $f(x)$, à coefficients rationnels, puisse être décomposé en facteurs du premier degré. Lorsqu'on aura trouvé ces symboles *nécessaires*, on devra naturellement les étudier d'une manière plus précise; c'est par cette étude que nous terminerons ces leçons.

Un exemple simple d'un problème analogue peut être donné au moment de l'introduction des nombres rationnels dans le calcul : Supposons qu'on introduise tous les nombres rationnels comme solutions des équations du premier degré $px+a=0$ où p et a sont entiers, p étant un nombre premier qui ne divise pas a; tous les symboles ainsi introduits seront distincts, mais on trouvera, ce que nous avons déjà indiqué, qu'il suffit d'introduire ceux qui vérifient les équations

$$px=1,$$

p étant un nombre premier, pour pouvoir les exprimer tous d'une façon explicite.

On peut d'ailleurs pour les nombres rationnels opérer synthétiquement, c'est-à-dire introduire précisément les symboles $\left(\frac{1}{p}\right)$ et montrer qu'ils suffisent ; mais dans le cas des nombres algébriques on verra plus loin combien une exposition synthétique parfaite serait pénible à cause de la complexité des liaisons qui existent entre ces symboles. Nous ajouterons néanmoins ici que cette exposition résultera naturellement des propriétés de l'ensemble des nombres algébriques auxquelles nous parviendrons plus tard.

Au sujet de cet ensemble, observons qu'un premier pas dans la classification de ses éléments peut être fait immédiatement. Les nombres algébriques qui vérifient une équation irréductible d'ordre n sont dits *nombres algébriques d'ordre* n, et il est clair que la définition précédente est *logique*, puisqu'un nombre algébrique vérifie une équation irréductible et une seule.

Une autre séparation des nombres algébriques apparaît également de suite :

Soit $a_0x^m+a_1x^{m-1}+\ldots+a_m=0$ une équation irréductible

d'ordre m à coefficients entiers; considérons la nouvelle équation

$$\varphi(y) = y^m + a_1 y^{m-1} + a_2 a_0 y^{m-2} + a_3 a_0^2 y^{m-3} + \cdots + a_m a_0^{m-1} = 0,$$

qu'on déduit de la première en multipliant ses deux membres par a_0^{m-1} et posant $a_0 x = y$. Cette nouvelle équation est évidemment irréductible et définit des nombres algébriques de même ordre que a précédente; à chaque racine y_i de la seconde équation correspond d'ailleurs une racine $x_i = \frac{y_i}{a_0}$ de la première, et réciproquement.

Les nombres algébriques qui satisfont à une équation irréductible à coefficients entiers, dont le premier terme a pour coefficient l'unité, sont dits *nombres algébriques entiers*. Cette définition nous permet de séparer en deux classes les nombres algébriques : ceux qui sont entiers et ceux qui ne le sont pas; ces derniers sont d'ailleurs les quotients des premiers par des nombres entiers ordinaires, de sorte que si l'on ne s'occupe que des symboles algébriques *nécessaires*, il suffit d'étudier les nombres algébriques entiers. Il est d'ailleurs facile de déduire de toute relation rationnelle entre des nombres algébriques une relation entre des nombres algébriques entiers, et réciproquement.

Ajoutons enfin qu'une relation entre des nombres algébriques entiers ne renfermera pas de nombres rationnels, puisque les seuls nombres algébriques entiers du premier ordre sont les nombres entiers ordinaires.

II. — Fonctions algébriques.

22. Nous avons vu qu'on a, en Algèbre élémentaire, introduit dans le calcul, des symboles de la forme $\frac{f(a, b, \ldots, l)}{g(a, b, \ldots, l)}$, f et g étant des polynomes, entiers par rapport aux variables indéterminées $a, b, \ldots, l$ et à coefficients rationnels. Ces symboles, qu'on appelle fractions rationnelles des variables $a, b, \ldots, l$, peuvent être, de la même manière que les polynomes à plusieurs variables, regardés comme définissant une *correspondance* entre les nombres rationnels, ou encore comme un moyen commode de considérer l'ensemble des nombres rationnels qu'on en déduit en remplaçant $a, b, \ldots, l$ par des nombres rationnels déterminés.

Le calcul de ces symboles a été défini en donnant à côté de la relation identique

$$g(a, b, \ldots, l) \cdot \frac{f(a, b, \ldots, l)}{g(a, b, \ldots, l)} = f(a, b, \ldots, l),$$

qui leur sert de définition, les propriétés de deux modes de composition : addition et multiplication, de ces symboles avec les polynomes entiers.

Il est possible de faire à l'égard des fractions rationnelles la même extension que celle qui a été faite en passant des nombres rationnels aux nombres algébriques.

Considérons un polynome entier en $x, a, b, \ldots, l$, à coefficients entiers, irréductible dans le *domaine d'intégrité* $[a, b, \ldots, l]$, et la relation

$$f(x, a, b, \ldots, l) = 0.$$

Il n'existe pas de fraction rationnelle en $a, b, \ldots, l$ qui, mise à la place de x, conduise à une identité en $a, b, \ldots, l$, sans quoi $f(x, a, b, \ldots, l)$ admettrait le diviseur du premier degré qui la définit. On introduira alors dans le calcul de nouveaux symboles vérifiant, par définition, cette relation et qu'on supposera se composer avec les polynomes suivant deux modes appelés toujours : addition et multiplication et possédant les propriétés de ces deux modes déjà supposées pour les fractions rationnelles. Ces nouveaux symboles sont appelés *fonctions algébriques des variables* $a, b, \ldots, l$.

Il est clair que si le degré du polynome irréductible considéré

$$f(x, a, b, \ldots, l)$$

est égal à n, il y aura n symboles qui seront définis simultanément, et ces n symboles, $X_1, X_2, \ldots, X_n$, vérifieront, lorsqu'on aura divisé le polynome donné par le coefficient de x^n, l'identité

$$f(x, a, b, \ldots, l) = (x - X_1)(x - X_2) \ldots (x - X_n).$$

Ajoutons que l'opération que l'on fait en introduisant ces symboles, c'est toujours l'extension du système formé par les fonctions rationnelles des variables $a, b, \ldots, l$ à coefficients rationnels, de façon que le polynome $f(x, a, b, \ldots, l)$ soit décomposable en facteurs linéaires dont les coefficients soient des éléments du nouveau système.

On voit donc nettement que l'étude des fonctions algébriques des variables $a, b, \ldots, l$ peut se faire d'une façon absolument parallèle

à celle des nombres algébriques, le point de départ étant l'ensemble des fonctions rationnelles à coefficients rationnels des variables $a, b, \ldots, l$ au lieu d'être l'ensemble des nombres rationnels. J'ajoute qu'aux nombres algébriques entiers, on peut faire correspondre les fonctions algébriques entières de $a, b, \ldots, l$, obtenues comme les symboles qui annulent un polynome entier en $x, a, b, \ldots, l$ à coefficients entiers, dont le premier coefficient est l'unité. On voit d'ailleurs immédiatement que les fonctions algébriques entières du premier ordre sont les polynomes entiers en $a, b, \ldots, l$ à coefficients entiers et que toute fonction algébrique des $a, b, \ldots, l$ est le quotient d'une fonction algébrique entière par un polynome entier en $a, b, \ldots, l$.

A un autre point de vue, une fonction algébrique des variables $a, b, \ldots, l$ peut représenter une *classe* de nombres algébriques, ceux que l'on obtient en remplaçant $a, b, \ldots, l$ par des nombres rationnels déterminés. Mais il est bien évident que les nombres algébriques ainsi obtenus peuvent être de nature très différente, suivant que la décomposition du polynome à coefficients déterminés qu'ils annulent est plus ou moins complète. La manière dont figurent, dans les coefficients, les indéterminées $a, b, \ldots, l$, n'a pas d'ailleurs une influence bien facile à préciser sur cette nature ; ce n'est que dans des cas extrêmement simples que la liaison apparaît nettement, et nous verrons que dans ces cas la considération des fonctions algébriques n'apporte de simplifications ni à l'écriture, ni à la manière d'exprimer les résultats.

Lorsque nous considérerons des fonctions algébriques de variables $a, b, \ldots, l$, nous les regarderons donc uniquement comme des symboles définis d'une manière analogue aux nombres algébriques et nous verrons qu'alors les propriétés des nombres algébriques, rapportées à l'ensemble des nombres rationnels, conduiront immédiatement aux propriétés des fonctions algébriques, rapportées à l'ensemble des fonctions rationnelles à coefficients rationnels de $a, b, \ldots, l$.

Enfin si on ne considère que les nombres algébriques entiers, leurs propriétés se transporteront, *mutatis mutandis*, aux fonctions algébriques entières dans le domaine d'intégrité $[a, b, \ldots, l]$.

Pour plus de précision et de netteté et afin d'introduire le moins d'arbitraires possible, nous commencerons par développer

uniquement l'étude des nombres algébriques, nous réservant de montrer plus tard comment les choses se passent pour les fonctions algébriques de plusieurs variables.

III. — Le théorème de d'Alembert.

23. Si l'on admet que les hypothèses faites pour définir les nombres algébriques n'entraînent pas de contradiction, ce qui sera démontré plus loin, les pages précédentes nous permettent de parler des nombres algébriques avec tout autant de liberté que des nombres entiers positifs, et en effet, pour nous, *les uns et les autres sont uniquement des symboles déterminés dont on connaît les modes de composition qui interviennent dans le calcul*, c'est-à-dire que *ce qu'on appelle calcul de ces symboles, n'est que le développement des deux modes de composition que nous savons étudier.*

Nous ne nous sommes pas encore préoccupés de l'existence d'objets représentés par nos symboles, du moins, pas jusqu'à présent pour les nombres algébriques ; nous allons le faire maintenant et nous observerons que cette existence mettra hors de doute qu'il n'existe pas de contradiction dans leur définition.

Comme on l'a déjà remarqué, on peut trouver de bien des manières des systèmes d'objets (ou d'opérations portant sur des objets) en nombre illimité et possédant les propriétés suivantes :

I. — On peut définir pour les objets un mode de composition conduisant de deux d'entre eux d'une manière unique à un troisième, et tel que :

1° La composition soit associative, commutative et *univoque* (le mot univoque est pris ici dans le sens le plus large : deux éléments d'une composition étant donnés, le troisième est déterminé d'une manière unique) ;

2° Il existe un objet d'effet nul dans cette composition : *objet nul.*

Cette composition sera nommée *addition.*

II. — On peut définir un mode de composition possédant les propriétés de la multiplication, c'est-à-dire tel que :

1° Le mode soit associatif, commutatif, *univoque* et distributif par rapport à l'addition ;

2° Il existe un objet d'effet nul dans la composition : *objet unité* ;

3° L'objet d'effet nul dans l'addition joue un rôle singulier ; il se reproduit par multiplication avec un objet quelconque.

On nommera le mode de composition précédent *multiplication.*

Lorsqu'on fixe un ensemble quelconque de tels objets, une question se pose naturellement : l'ensemble des objets est-il *équivalent* à l'ensemble des symboles ? En d'autres termes, peut-on faire correspondre à chaque objet un symbole et à chaque symbole un objet de façon que la correspondance se conserve lorsqu'on exécute sur les objets et les symboles des opérations correspondantes ?

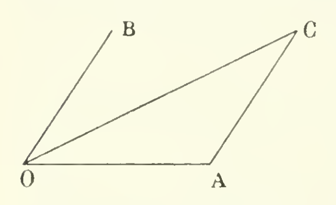
Si les objets sont des grandeurs à signe, on a déjà vu qu'on avait la représentation des nombres négatifs entiers; si l'on admet de plus leur divisibilité en parties égales, on a la représentation des nombres rationnels. On peut d'ailleurs représenter également les polynomes à une ou plusieurs indéterminées.

Considérons maintenant une équation irréductible déterminée,

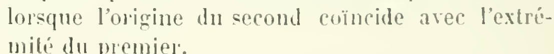
$$f(x) = 0 ;$$

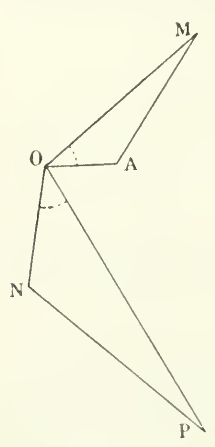
on peut, *dans le système d'objets donné, demander s'il existe ou non des racines,* c'est-à-dire rechercher s'il y a ou non des objets du système qui, composés avec eux-mêmes ainsi que l'indique le polynome $f(x)$, donnent l'objet d'effet nul dans l'addition. Il est clair que la réponse à cette question dépend du système d'objets qu'on se donne et que la question est plutôt du ressort des mathématiques appliquées que des mathématiques pures.

Le théorème de d'Alembert est une proposition qui permet de répondre affirmativement à la question dont on vient de parler, pour *certains* systèmes d'objets, en particulier pour les *segments* situés dans un plan.



Considérons en effet les segments situés dans un plan, c'est-à-dire des éléments ayant à la fois une longueur, une direction et un sens; nous regarderons deux segments parallèles de même longueur et de même sens comme étant le même objet, c'est-à-dire que l'origine d'un segment est indéterminée. Le segment nul sera celui dont l'origine et l'extrémité coïncident.

On définira la *somme* de deux segments OA et OB comme le segment OC qui a même origine que le premier et même extrémité que le second,  lorsque l'origine du second coïncide avec l'extrémité du premier.



Pour définir la multiplication, nous supposerons qu'un segment donné OA a été pris comme unité; le *produit* d'un segment OM par un segment ON est alors un segment OP tel que les triangles OAM et ONP soient semblables et disposés de même. La disposition est définie, on le sait, par la succession des éléments : côtés et angles.

On a supposé dans les définitions précédentes de la somme et du produit que les segments considérés avaient même origine; il est inutile d'ajouter que c'est là une hypothèse légitime d'après la définition donnée d'un segment, et il serait facile d'établir que les opérations ainsi définies satisfont bien aux neuf conditions indiquées plus haut.

Le théorème de d'Alembert peut alors s'énoncer de la manière suivante : *Etant donnée une équation algébrique entière d'ordre n,* $f(x) = 0$,

dont les coefficients représentent des segments quelconques, il existe toujours n segments qui la vérifient, c'est-à-dire qui, composés avec eux-mêmes et les segments coefficients, comme l'indique le polynome $f(x)$, conduisent au segment zéro.

C'est là un théorème de *pure géométrie*, théorème qui est en outre *très spécial*, puisqu'il faut démontrer un théorème analogue pour chaque ensemble d'objets qui peuvent être représentés par nos symboles.

Remarquons d'ailleurs du théorème de d'Alembert qu'il prouve l'existence de n segments dont les fonctions symétriques élémentaires sont des segments quelconques donnés à l'avance. Nous verrons plus tard qu'en Algèbre, c'est-à-dire dans l'étude des symboles algébriques, il suffit d'établir le fait lorsque les segments donnés sont des segments rationnels ou entiers, la proposition s'étendant d'elle-même à n segments *algébriques*, mais qu'on n'a jamais à considérer des segments *quelconques*.

Il arrive en effet généralement que lorsqu'on choisit n segments quelconques, il est impossible de choisir le segment unité de façon que les autres soient rationnels ou algébriques. Le théorème de d'Alembert sort donc, même avec l'interprétation précise que nous lui donnons, du domaine de l'Algèbre entendue comme l'étude des symboles algébriques.

Il est presque inutile d'ajouter ici que toutes les démonstrations *rigoureuses* qu'on a données de ce théorème au point de vue où nous nous plaçons, en particulier celle de Cauchy, peuvent aisément être rendues purement géométriques. Nous renverrons le lecteur aux ouvrages connus pour vérifier ce point. Nous ne donnerons ici la démonstration du théorème que dans le cas extrêmement simple où $f(x)$ est du second degré ; elle ne fait alors appel qu'à des considérations immédiates de Géométrie élémentaire.

On peut évidemment supposer $f(x)$ mis sous la forme $x^2 - p_1x + p_2$, p_1 et p_2 étant des segments déterminés, mais quelconques. Il est clair que si l'on pose $x = y + \frac{1}{2}p_1$, la détermination de y dépendra de la relation

$$y^2 = \frac{p_1^2}{4} - p_2.$$

Mais on sait construire le segment $\frac{p_1^2}{4} - p_2$, désignons-le par a ; il restera à déterminer le segment y qui vérifie la relation

$$y^2 = a.$$

On observe que la droite issue de l'origine sur laquelle il sera situé est la bissectrice de l'angle formé par le segment a et le segment unité ; sa longueur sera d'ailleurs une moyenne proportionnelle entre les longueurs des segments a et 1 ; on a appris à la construire en géométrie élémentaire.

Les deux segments η et $-\eta$ qu'on obtient ainsi, vérifient évidemment tous deux la relation $y^2 = a$; il suffira de leur ajouter le segment $\frac{1}{2}p_1$ pour

obtenir deux segments ξ_1 et ξ_2 vérifiant la relation $x^2 - p_1 x + p_2 = 0$. Le théorème est donc démontré dans le cas du second degré.

IV. — Les fonctions symétriques.

24. Il résulte manifestement de l'introduction des nombres algébriques dans le calcul que *tout polynome entier en x de degré n à coefficients rationnels, peut s'écrire et d'une seule manière sous forme d'un produit de n facteurs du premier degré en x, à coefficients algébriques.*

Si l'on a en effet, en décomposant le polynome $f(x)$ en facteurs irréductibles,

$$f(x) = g^\alpha(x) . h^\beta(x) \, .. \, l^\lambda(x),$$

on voit que dans $f(x)$, les facteurs du premier degré $(x - \xi)$ correspondant aux racines ξ de l'équation $g(x) = 0$ figureront à la puissance α, les facteurs $(x - \eta)$ correspondant aux racines de $h(x) = 0$ figureront à la puissance β, etc. La théorie de la divisibilité des polynomes montre qu'il n'existe pas d'autre décomposition de $f(x)$ en facteurs du premier degré.

La relation $f(x) = 0$, dans laquelle on ne suppose rien sur la réductibilité du polynome $f(x)$, et lorsqu'on la considère comme définissant les nombres algébriques qui la vérifient, s'appelle, comme l'on sait, une *équation algébrique*. Les n nombres algébriques $x_1, x_2, .. , x_n$ dont plusieurs peuvent être égaux et qui vérifient l'identité en x,

$$f(x) = (x - x_1)(x - x_2) \dots (x - x_n),$$

sont dits les *racines* de cette équation.

A l'égard de ces nombres on peut observer qu'en décomposant $f(x)$ en facteurs irréductibles, il est toujours possible de *former une équation qui admette pour racines tous les nombres différents de la suite* $x_1, x_2, \dots, x_n$; cette équation est manifestement

$$g(x) . h(x) \dots . \, l(x) = 0.$$

Nous ferons remarquer, néanmoins, qu'il n'est nullement nécessaire de décomposer $f(x)$ en ses facteurs irréductibles pour arriver à ce résultat et nous allons pour l'établir donner ici une notion importante, celle de *polynome dérivé* d'un polynome.

25. Considérons un polynome de degré n à coefficients rationnels,

$$f(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n.$$

et remplaçons dans ce polynome x par $x+h$; nous obtiendrons, en ordonnant le résultat suivant les puissances croissantes de h, la nouvelle identité en x et h,

$$f(x+h) = f(x) + \frac{h}{1} f'(x) + \frac{h^2}{1.2} f''(x) + \cdots + \frac{h^n}{1.2\ldots n} \cdot f^n(x),$$

$f'(x)$, $f''(x)$,.. désignant les polynomes suivants :

$$f'(x) = na_0x^{n-1} + (n-1)a_1x^{n-2} + \cdots + a_{n-1},$$

$$f''(x) = n(n-1)a_0x^{n-2} + (n-1)(n-2)a_1x^{n-3} + \cdots + 2.a_{n-2},$$

. . . .

$$f^n(x) = n(n-1)(n-2)\ldots 2.1.a_0.$$

On observe que le polynome $f''(x)$ se déduit du polynome $f'(x)$ en opérant sur ce dernier comme on a opéré sur $f(x)$ pour obtenir $f'(x)$. On dit que le polynome $f'(x)$ est le *dérivé* du polynome $f(x)$; le polynome $f''(x)$ qui est le dérivé de $f'(x)$ sera dit alors *polynome dérivé second* de $f(x)$, etc. Il convient de remarquer que si les coefficients du polynome $f(x)$ sont entiers, ceux de ses divers dérivés le sont également.

Cela étant acquis, il est clair que si un polynome $f(x)$ est irréductible, il est premier avec le polynome dérivé $f'(x)$; un polynome irréductible est, en effet, premier avec tout polynome entier de degré inférieur au sien.

Considérons ensuite un produit de deux polynomes irréductibles $f(x)$ et $g(x)$ supposés différents, polynomes qui sont évidemment premiers entre eux, et formons le polynome dérivé du produit $F(x) = f(x).g(x)$. C'est, par définition, le coefficient de h dans le produit $f(x+h).g(x+h)$, et comme l'on a

$$f(x+h) = f(x) + \frac{h}{1} f'(x) + \frac{h^2}{1\,2} f''(x) + \cdots,$$

$$g(x+h) = g(x) + \frac{h}{1} g'(x) + \frac{h^2}{1.2} g''(x) + \cdots,$$

il en résulte

$$F'(x) = f(x).g'(x) + g(x).f'(x).$$

On peut affirmer que $F(x)$ est premier avec $F'(x)$. En effet, pour qu'un des facteurs $g(x)$ de $F(x)$ divise $f(x).g'(x) + g(x).f'(x)$, il faut et il suffit qu'il divise $f(x).g'(x)$; or $g(x)$ est premier avec $f(x)$ et avec $g'(x)$; donc il est premier avec leur produit.

La proposition s'étend immédiatement à un nombre quelconque de facteurs irréductibles différents, d'où il résulte que :

Tout polynome qui n'admet que des diviseurs distincts est premier avec le polynome dérivé.

Soit au contraire un produit $f^{\alpha}(x)$ de α facteurs irréductibles identiques ; le coefficient de h dans l'expression $f^{\alpha}(x+h)$, c'est-à-dire dans le développement de $\left[f(x)+\frac{h}{1}f'(x)+\frac{h^2}{1.2}f''(x)\ldots\right]^{\alpha}$, est manifestement $\alpha f^{\alpha-1}(x) f'(x)$. Comme $f(x)$ et $f'(x)$ sont premiers entre eux, $f^{\alpha}(x)$ admet avec le polynome dérivé le plus grand commun diviseur $f^{\alpha-1}(x)$.

On conclut de là que *tout polynome* F *qui, décomposé en facteurs irréductibles, a la forme*

$$F = f^{\alpha}.\, g^{\beta} \ldots l^{\lambda},$$

admet avec le polynome dérivé F' *un plus grand commun diviseur*

$$D = f^{\alpha-1}.\, g^{\beta-1} \ldots l^{\lambda-1},$$

et par suite qu'*après division de* F *par ce plus grand commun diviseur on obtient un polynome dont tous les facteurs irréductibles sont distincts.*

Il suffira par conséquent pour passer d'une équation $f(x)=0$ à une équation admettant seulement les racines distinctes de la première, de diviser $f(x)$ par le plus grand commun diviseur entre $f(x)$ et $f'(x)$ et d'égaler à zéro le quotient obtenu.

26. Considérons donc une équation $f(x)=0$ dont toutes les racines sont distinctes.

Si l'on pose

$$f(x) = x^n - p_1 x^{n-1} + p_2 x^{n-2} \cdots \pm p_n,$$

on obtiendra entre les coefficients $p_1, p_2, \ldots, p_n$ et les racines $x_1, \ldots, x_n$, les relations fondamentales bien connues :

$$x_1 + x_2 + \cdots + x_n = p_1,$$
$$x_1 x_2 + \cdots + x_{n-1} x_n = p_2,$$
$$\ldots\ldots\ldots\ldots$$
$$x_1 x_2 \ldots\ldots\ldots x_n = p_n.$$

On les énonce en disant que *lorsque le coefficient de x^n est l'unité, les*

coefficients de l'équation sont, au signe près, les fonctions symétriques élémentaires des racines.

Nous allons étudier d'une manière plus générale des fractions rationnelles de $x_1, x_2, \ldots, x_n$ symétriques par rapport à ces lettres, c'est-à-dire qui ne changent point lorsqu'on y remplace respectivement x_i par x_k et x_k par x_i, quels que soient i et k choisis dans la suite $1, 2, \ldots, n$. A leur sujet nous établirons *sous la seule condition que $x_1, x_2, \ldots, x_n$ soient des symboles différents capables de se composer entre eux et avec les nombres rationnels en suivant les lois de l'addition et de la multiplication des entiers*, les deux propositions suivantes : *Toute fraction rationnelle symétrique de $x_1, x_2, \ldots, x_n$ à coefficients rationnels est le quotient de deux polynomes* SYMÉTRIQUES *en $x_1, x_2, \ldots, x_n$ à coefficients entiers ;*

Tout polynome symétrique en $x_1, x_2, \ldots, x_n$ à coefficients entiers peut s'exprimer d'une seule manière comme polynome entier en $p_1, p_2, \ldots, p_n$ à coefficients entiers ; $p_1, p_2, \ldots, p_n$ étant toujours les fonctions symétriques élémentaires de $x_1, x_2, \ldots, x_n$.

Soit $\dfrac{f(x_1, x_2, \ldots, x_n)}{g(x_1, x_2, \ldots, x_n)}$ une fraction symétrique rationnelle *irréductible*, c'est-à-dire telle que les deux polynomes f et g, qu'on peut évidemment supposer à coefficients entiers, décomposés en facteurs irréductibles, n'aient aucun facteur commun. Je vais montrer que f et g sont des fonctions symétriques entières. En effet, d'après la définition même d'une fonction symétrique, $\dfrac{f}{g}$ ne doit pas changer lorsqu'on échange entre elles deux des lettres $x_1, \ldots, x_n$, par exemple x_1 et x_2. On a donc l'identité

$$\frac{f(x_1, x_2, \ldots x_n)}{g(x_1, x_2, \ldots x_n)} = \frac{f(x_2, x_1, \ldots x_n)}{g(x_2, x_1, \ldots x_n)} = \frac{f(x_1, x_2, \ldots x_n) - f(x_2, x_1, \ldots x_n)}{g(x_1, x_2, \ldots x_n) - g(x_2, x_1, \ldots x_n)}.$$

La différence $f(x_1, x_2, \ldots, x_n) - f(x_2, x_1, \ldots, x_n)$ est un polynome entier en x_1 qui devient égal à zéro lorsqu'on y remplace x_1 par x_2 ; *s'il ne se réduit pas à zéro*, il est donc divisible par $x_1 - x_2$; il en est de même de la différence

$$g(x_1, x_2, \ldots, x_n) - g(x_2, x_1, \ldots, x_n).$$

On peut donc, en supprimant ce facteur commun $x_1 - x_2$, écrire l'identité

$$\frac{f}{g} = \frac{f'}{g'},$$

f' et g' étant des polynomes en $x_1, x_2, \ldots, x_n$ qui sont en x_1 et x_2 de degrés respectivement inférieurs aux degrés de f et de g ; or une telle identité est impossible puisqu'on a supposé $\frac{f}{g}$ irréductible. On conclut de là que la différence

$$f(x_1, x_2, \ldots, x_n) - f(x_2, x_1, \ldots, x_n)$$

se réduit à zéro, et comme cela a lieu quelles que soient les lettres x_1, x_2 choisies, la fonction f est symétrique. Il en sera de même de la fonction g.

La remarque précédente fait voir qu'*on n'a besoin d'étudier que les fonctions symétriques entières à coefficients entiers de* $x_1, x_2, \ldots, x_n$. Soit donc $F(x_1, x_2, \ldots, x_n)$ une telle fonction ; nous allons montrer qu'elle s'exprime, et d'une seule manière, comme fonction entière à coefficients entiers de $p_1, p_2, \ldots, p_n$.

La fonction F est une somme de termes de la forme $Ax_1^{\alpha_1}x_2^{\alpha_2}\ldots x_n^{\alpha_n}$, $\alpha_1, \alpha_2, \ldots, \alpha_n$ étant des entiers positifs et A un entier ; désignons par g un entier positif supérieur à la plus grande des sommes $\alpha_1 + \alpha_2 + \cdots + \alpha_n$ et faisons dans $p_1, p_2, \ldots, p_n$ la substitution $x_i = x^{g^{i-1}}$.

Les polynomes en $x_1, x_2, \ldots, x_n$ que nous avons désignés par $p_1, p_2, \ldots, p_n$ deviendront des polynomes à une variable x, et les termes de degré le plus élevé en x seront respectivement dans ces polynomes, des termes en

$$x^{g^{n-1}}, \qquad x^{g^{n-2}+g^{n-1}}, \qquad \ldots\ldots \qquad \text{et} \qquad x^{g^0+g^1+g^2+\cdots+g^{n-1}}.$$

Si maintenant nous considérons le polynome F, le terme

$$Ax_1^{\alpha_1}x_2^{\alpha_2}\ldots\ldots x_n^{\alpha_n}$$

deviendra $Ax^{\alpha_n g^{n-1}+\alpha_{n-1}g^{n-2}+\cdots+\alpha_1 g^0}$, et d'après la manière même dont on a choisi g il n'y a aucune réduction possible entre les termes du polynome à une variable ainsi obtenu. Ces termes correspondent donc d'une manière univoque et réciproque aux termes de $F(x_1, x_2, \ldots, x_n)$. Or on peut ranger les termes du polynome à une variable dans un ordre déterminé, par exemple en l'ordonnant par rapport aux puissances décroissantes de x ; il en sera par suite de même pour $F(x_1, x_2, \ldots, x_n)$. Considérons en particulier le terme $Ax_1^{\alpha_1}x_2^{\alpha_2}\ldots\ldots x_n^{\alpha_n}$; puisque la fonction F est symétrique, elle renferme aussi les termes qu'on déduit de celui-là en y permutant d'une

manière quelconque les x ; parmi tous ces termes celui qui sera rangé le premier sera évidemment un de ceux pour lesquels les entiers de la suite $\alpha_1, \alpha_2, \ldots, \alpha_n$ ne vont jamais en décroissant. Supposons que ce terme donne le terme de degré le plus élevé du polynome à une variable ; nous retrancherons de $F(x_1, x_2, \ldots, x_n)$ le terme $Ap_1^{\beta_1}p_2^{\beta_2}\ldots\ldots p_n^{\beta_n}$, dans lequel $\beta_1, \ldots, \beta_n$ sont déterminés d'une manière unique par les relations

$$\beta_n = \alpha_1,$$

$$\beta_{n-1} + \beta_n = \alpha_2,$$

$$\ldots\ldots\ldots\ldots\ldots,$$

$$\beta_1 + \beta_2 \ldots + \beta_n = \alpha_n,$$

c'est-à-dire où l'on a $\beta_{n-i} = \alpha_{i+1} - \alpha_i$, les lettres $p_1, p_2, \ldots, p_n$ étant remplacées par leur expression en $x_1, x_2, \ldots, x_n$.

On fera ainsi disparaître le terme de $F(x_1, x_2, \ldots, x_n)$ qui donne le premier terme du polynome à une variable correspondant. Si l'on remarque qu'en transformant $Ap_1^{\beta_1}p_2^{\beta_2}\ldots\ldots p_n^{\beta_n}$ en un polynome à une variable, le terme considéré est celui qui est de degré le plus élevé, on voit qu'on a abaissé le degré du polynome à une variable correspondant à la fonction $F(x_1, x_2, \ldots. x_n)$.

En opérant sur le polynome à une variable déduit de

$$F - Ap_1^{\beta_1}p_2^{\beta_2}\ldots\ldots p_n^{\beta_n}$$

comme sur F, et ainsi de suite, on parviendra évidemment et d'une seule manière à une expression indépendante des x. On pourra donc écrire

$$F = \Sigma Ap_1^{\beta_1}p_2^{\beta_2}\ldots\ldots p_n^{\beta_n},$$

et les coefficients du second membre seront manifestement entiers en même temps que ceux du premier.

Il reste à démontrer qu'il n'existe pas une seconde manière de ramener F à une fonction entière de $p_1, p_2, \ldots, p_n$, c'est-à-dire au fond *qu'il n'existe pas de fonction entière de* $p_1, p_2, \ldots, p_n$ *qui soit nulle quels que soient les* x, *sans être aussi nulle quels que soient les* p. Admettons que l'on ait entre les x l'identité

$$\Sigma Ap_1^{\beta_1}p_2^{\beta_2}\ldots\ldots p_n^{\beta_n} = \Sigma A'p_1^{\beta_1'}p_2^{\beta_2'}\ldots\ldots p_n^{\beta_n'}.$$

La transformation $x_i = x^{g^{i-1}}$ fera correspondre aux deux membres des polynomes entiers en x qui seront également identiques.

Considérons le terme $Ap_1^{\beta_1}p_2^{\beta_2}\ldots p_n^{\beta_n}$, qui conduit au terme de degré le plus élevé du polynome en x correspondant et le terme analogue $A'p_1^{\beta'_1}p_2^{\beta'_2}\ldots\ldots p_n^{\beta'_n}$ du second membre.

On aura évidemment, puisque ces termes de plus haut degré sont identiques,

$$A = A'$$

et ensuite

$$\begin{aligned}\beta_1 g^{n-1} + \beta_2(g^{n-2} + g^{n-1}) + \cdots + \beta_n(g^0 + g^1 + \cdots + g^{n-1})\\ = \beta'_1 g^{n-1} + \beta'_2(g^{n-2} + g^{n-1}) + \cdots + \beta'_n(g^0 + g^1 + \cdots + g^{n-1}),\end{aligned}$$

ce qui peut s'écrire

$$\begin{aligned}\beta_n g^0 + (\beta_n + \beta_{n-1})g^1 + \cdots + (\beta_n + \beta_{n-1} + \cdots + \beta_1)g^{n-1}\\ = \beta'_n g^0 + (\beta'_n + \beta'_{n-1})g_1 + \cdots + (\beta'_n + \beta'_{n-1} + \cdots + \beta'_1)g^{n-1}.\end{aligned}$$

Cette relation ayant lieu quel que soit g, supposé choisi supérieur à un certain nombre, on en déduit

$$\begin{gathered}\beta_n = \beta'_n,\\ \beta_n + \beta_{n-1} = \beta'_n + \beta'_{n-1},\\ \dots\dots\dots\dots\dots\\ \beta_n + \cdots + \beta_1 = \beta'_n + \cdots + \beta'_1,\end{gathered}$$

c'est-à-dire que les β sont identiques aux β'. Le raisonnement se continue après suppression des deux termes identiques et la proposition est par conséquent démontrée.

La méthode précédente pour le calcul des fonctions symétriques est connue sous le nom de méthode de Waring.

V. — Propriétés générales des nombres algébriques.

27. Les propositions établies sur les fonctions symétriques de $x_1, x_2, \ldots, x_n$ vont être appliquées à l'étude d'une question qu'on peut poser immédiatement après l'introduction des symboles algébriques : Nous avons vu qu'avec les nombres algébriques $\xi_1, \xi_2, \ldots, \xi_n$ s'introduisaient nécessairement dans le calcul toutes les fractions rationnelles de $\xi_1, \xi_2, \ldots, \xi_n$ à coefficients rationnels ; il est donc intéressant de savoir quelle est la nature de ces éléments, c'est-à-dire comment chacun d'eux est lié aux nombres rationnels.

Nous allons rechercher d'une manière plus générale la nature des fonctions de nombres algébriques donnés que l'on sait définir jusqu'à présent, c'est-à-dire des polynomes entiers, des fractions rationnelles et des fonctions algébriques ; mais pour plus de précision nous nous bornerons à considérer des nombres algébriques *entiers*. Nous avons en effet observé que toute relation entre de tels nombres se transforme immédiatement en une relation entre des nombres algébriques quelconques, et réciproquement : nous verrons d'ailleurs que les propositions auxquelles on parvient ainsi seront les généralisations naturelles de celles obtenues dans l'étude des nombres entiers ordinaires.

Désignons par $f(x) = 0$ une équation irréductible d'ordre n à coefficients entiers, le premier d'entre eux étant l'unité, et soit ξ l'une de ses racines, c'est-à-dire un nombre algébrique entier déterminé d'ordre n ; proposons-nous d'étudier la *nature des fonctions rationnelles de* ξ, *à coefficients rationnels.* On sait qu'une telle fonction se ramène toujours, à l'aide de la relation $f(\xi)=0$, à un polynome entier en ξ à coefficients rationnels, de degré inférieur à n ; il suffit donc de considérer ces polynomes et même les polynomes à coefficients entiers dont les premiers dérivent immédiatement. Soit donc $g(\xi)$ un polynome entier en ξ à coefficients entiers de degré inférieur à n ; désignons par $\xi_1 = \xi, \xi_2, \xi_3, \ldots, \xi_n$ les racines de $f(x)$ qui sont distinctes, comme l'on sait. Il est clair que si l'on considère le produit

$$\Phi(z) = [z - g(\xi_1)].[z - g(\xi_2)].\ldots.[z - g(\xi_n)]$$

étendu à toutes les racines de $f(x)$, ce produit est un polynome entier en z dont les coefficients sont entiers, le premier étant l'unité, puisqu'ils sont symétriques en $\xi_1, \xi_2, \ldots, \xi_n$. Or ce produit s'annule en particulier pour $z = g(\xi)$; on conclut de là que $g(\xi)$ *est un nombre algébrique entier, d'ordre au plus égal au degré de* Φ, *c'est-à-dire à* n.

Si l'équation $\Phi(z) = 0$ est irréductible, on peut affirmer que $g(\xi)$ est un nombre algébrique d'ordre n. Sinon, soit $\varphi(z)$ un facteur irréductible de $\Phi(z)$; $\varphi(z)$ s'annule pour une des valeurs de $g(\xi)$, c'est-à-dire que l'équation $\varphi[g(x)] = 0$ et l'équation $f(x) = 0$ ont une racine commune. Comme $f(x)$ est irréductible, il en résulte que $\varphi[g(x)]$ est divisible par $f(x)$, c'est-à-dire en d'autres termes

que $\varphi(z)$ s'annule pour toutes les déterminations distinctes de $g(\xi)$. Il est clair que $\varphi(z)$ ne peut s'annuler pour d'autres déterminations de z, donc tous les facteurs irréductibles de $\Phi(z)$ sont identiques. On a par suite

$$\Phi(z) = [\varphi(z)]^p,$$

et si l'on désigne par k le degré de $\varphi(z)$: $n = kp$. *L'ordre du nombre algébrique entier $g(\xi)$ est donc toujours un diviseur de l'ordre de ξ.*

28. Nous avons reconnu que les polynomes en ξ d'ordre inférieur à n et à coefficients entiers sont des nombres algébriques entiers de différents ordres, ces ordres étant toujours des diviseurs du degré de l'équation irréductible qui définit ξ ; on dit que l'ensemble de ces polynomes en ξ à coefficients entiers constitue un *domaine algébrique d'intégrité* et l'on désigne ce domaine par $[\xi]$.

Essayons d'approfondir un peu plus la dépendance qui existe entre les polynomes irréductibles $f(x)$ et $\varphi(z)$ qui s'annulent pour deux éléments ξ et $g(\xi)$ du domaine $[\xi]$.

Admettons toujours que $g(\xi)$ soit un nombre algébrique entier d'ordre k ; nous savons que parmi les expressions $g(\xi_1)$, $g(\xi_2)$, . . ., $g(\xi_n)$, k seulement sont distinctes ; nous pouvons supposer que ces expressions sont précisément

$$g(\xi_1),\ g(\xi_2),\ \ldots,\ g(\xi_k)$$

et nous rangerons les autres de telle sorte que l'on ait

$$g(\xi_j) = g(\xi_i),$$

sous la seule condition $j = i + mk$, m étant un entier quelconque.

Considérons alors l'équation en ξ : $g(\xi) - g(\xi_i) = 0$; elle admet évidemment toutes les racines ξ_j telles que $j = i + mk$ et n'en admet pas d'autres. Par conséquent le plus grand commun diviseur entre $g(x) - g(\xi_i)$ et le polynome $f(x)$ est le produit $\prod_j (x - \xi_j)$ dans lequel $j = i + mk$. Si nous désignons par $h[x, g(\xi_i)]$ ce produit, on pourra écrire

$$f(x) = \prod_{i=1}^{i=k} h[x, g(\xi_i)].$$

Cette formule montre que l'équation $f(x) = 0$, qui est irréductible, admet le facteur $h[x, g(\xi_i)]$ si l'on désigne par $g(\xi_i)$ une racine

de l'équation qui définit $g(\xi)$, c'est-à-dire une racine de $\varphi(z) = 0$. On énonce habituellement ce résultat en disant que *dans le domaine d'intégrité $g(\xi)$, l'équation $f(x) = 0$ est réductible*, ou en d'autres termes que *l'adjonction du nombre algébrique entier $g(\xi)$ à l'ensemble des nombres entiers permet de décomposer le polynome $f(x)$ en deux facteurs dont l'un est $h[x, g(\xi)]$.*

29. Passons à la considération des fractions rationnelles, à coefficients rationnels, de nombres algébriques entiers donnés. De telles expressions étant le quotient de deux polynomes entiers à coefficients entiers, nous commencerons par étudier ces polynomes. Supposons donc que $\xi, \eta, \zeta, \ldots$ soient des nombres algébriques entiers qui vérifient chacun l'une des équations irréductibles à coefficients entiers

$$f(x) = 0, \qquad g(y) = 0, \qquad h(z) = 0, \qquad \ldots,$$

équations qui sont respectivement de degrés $l, m, n, \ldots$, et considérons un polynome entier à coefficients entiers $P(\xi, \eta, \zeta, \ldots)$. On peut évidemment l'amener en tenant compte des définitions de $\xi, \eta, \zeta, \ldots$, à ne renfermer ξ qu'au degré $l-1$ au plus, η qu'au degré $m-1$, etc., sans que ses coefficients cessent d'être entiers. Si l'on effectue alors le produit

$$\prod_{i=1}^{i=l} [u - P(\xi_i, \eta, \zeta, \ldots)]$$

on obtiendra un polynome entier en u dont tous les coefficients sont des polynomes entiers en $\eta, \zeta, \ldots$ à coefficients entiers, sauf le premier qui est l'unité, polynome qui s'annule pour $u = P(\xi, \eta, \zeta, \ldots)$. Désignons par $P_1(u, \eta, \zeta, \ldots)$ ce polynome et formons le produit

$$\prod_{i=1}^{i=m} P_1(u, \eta_i, \zeta, \ldots)$$

ce produit ne renfermera plus ni ξ ni η, et s'annulera toujours pour

$$u = P(\xi, \eta, \zeta, \ldots).$$

Il est clair qu'on parviendra ainsi à un polynome entier en u à coefficients entiers, le premier étant l'unité, c'est-à-dire que le sym-

bole $P(\xi, \eta, \zeta, \ldots)$ qui annule ce polynome, est un nombre algébrique entier. L'ordre de ce nombre est d'ailleurs au plus égal au produit des ordres des nombres algébriques $\xi, \eta, \zeta, \ldots$, et il serait aisé de montrer qu'il est toujours un diviseur de ce produit.

On peut donc dire que *toute fonction entière à coefficients entiers de nombres algébriques entiers est un nombre algébrique entier.*

Toute fraction rationnelle de plusieurs nombres algébriques entiers se ramène donc à la forme $\frac{\alpha_1}{\beta_1}$, α_1 et β_1 étant deux nombres algébriques entiers que l'on sait définir. Si l'on désigne par $\beta_2, \beta_3, \ldots, \beta_n$ les nombres algébriques *conjugués* de β, c'est-à-dire les autres racines de l'équation irréductible à coefficients entiers que vérifie β, on a évidemment

$$\frac{\alpha_1}{\beta_1} = \frac{\alpha_1 \cdot \beta_2 \cdot \beta_3 \ldots \beta_n}{\beta_1 \cdot \beta_2 \cdot \beta_3 \ldots \beta_n},$$

c'est-à-dire que $\frac{\alpha_1}{\beta_1}$ est le quotient d'un nombre algébrique entier par un nombre entier. Toute fraction rationnelle de plusieurs nombres algébriques entiers est donc un nombre algébrique, qui n'est généralement pas un nombre algébrique entier.

30. Considérons maintenant un polynome entier en x dont les coefficients sont des fonctions entières des nombres algébriques entiers $\xi, \eta, \zeta, \ldots$ Soit $P(x, \xi, \eta, \zeta, \ldots)$ ce polynome ; on peut se poser à son égard la question déjà posée à l'égard des polynomes à coefficients rationnels : Existe-t-il des nombres rationnels ou algébriques x_0 qui, mis à la place de x, donnent l'identité

$$P(x_0, \xi, \eta, \zeta, \ldots) = 0.$$

Il suffit de se reporter aux raisonnements du paragraphe précédent, pour conclure, de la relation $P(x_0, \xi, \eta, \zeta \ldots) = 0$, une relation à coefficients entiers :

$$R(x_0) = 0,$$

c'est-à-dire que le nombre x_0 est l'une des racines de l'équation $R(x) = 0$. Il résulte d'ailleurs de la théorie de la divisibilité qu'il existe un nombre de racines de l'équation $R(x) = 0$ égal au degré du polynome $P(x, \xi, \eta, \zeta, \ldots)$ qui annulent ce polynome, c'est-à-dire que *tout polynome entier en x, à coefficients algébriques, s'an-*

nulle pour un nombre de déterminations algébriques de x, égal à son degré.

Si l'on suppose en outre que le coefficient de la plus haute puissance de x dans $P(x, \xi, \eta, \zeta, \ldots)$ soit l'unité, on voit qu'il en sera de même dans $R(x)$, c'est-à-dire que *les nombres algébriques qui annulent le polynome* $P(x, \xi, \eta, \zeta, \ldots)$ *dont les coefficients sont des nombres algébriques entiers, le premier étant l'unité, sont des nombres algébriques entiers.*

Considérons, par exemple, le cas simple d'un polynome entier en y, dont les coefficients, sauf le premier qui est l'unité, sont des fonctions entières à coefficients entiers d'un seul nombre algébrique entier ξ, racine de l'équation irréductible $f(x) = 0$. Si l'on désigne par $g(y, \xi)$ ce polynome, on peut se proposer de *chercher quels sont les nombres algébriques entiers qui vérifient l'équation*

$$g(y, \xi) = 0.$$

Nous formerons à cet effet le produit $\prod g(y, \xi_i)$ étendu à toutes les racines $\xi_1, \xi_2, \ldots, \xi_n$ de $f(x)$ et nous désignerons ce produit, qui est un polynome entier en y à coefficients entiers, par $G(y)$. On sait décomposer $G(y)$ en facteurs irréductibles, soit

$$G(y) = H^{\alpha}(y) . H_1^{\alpha_1}(y) \ldots\ldots$$

la décomposition obtenue ; la relation

$$\prod g(y, \xi_i) = H^{\alpha}(y) . H_1^{\alpha_1}(y) \ldots\ldots$$

montre que l'équation $H(y) = 0$ admet nécessairement une racine au moins de l'une des équations $g(y, \xi_i) = 0$, c'est-à-dire que les polynomes $H(y)$ et $g(y, \xi_i)$ admettent un plus grand diviseur commun renfermant y. Soit $d(y, \xi_i)$ ce plus grand diviseur commun dont les coefficients, sauf le premier qui est l'unité, sont fonctions entières à coefficients entiers de ξ_i ; on peut écrire les identités en y :

$$H(y) = d(y, \xi_i) . k(y, \xi_i),$$

$$g(y, \xi_i) = d(y . \xi_i) . l(y . \xi_i),$$

et ces identités conduisant à des relations entières en ξ_i à coefficients entiers sont vérifiées, d'après une proposition connue, par toutes les racines de l'équation irréductible $f(x) = 0$.

Il en résulte que $H(y)$ admet nécessairement un diviseur commun $d(y, \xi)$ avec $g(y, \xi)$ et que ce diviseur est leur plus grand diviseur commun. On peut donc dire que *parmi les racines de* $g(y, \xi) = 0$, *celles qui vérifient la relation* $d(y, \xi) = 0$ *sont des racines de l'équation irréductible à coefficients entiers* $H(y) = 0$. Si l'on opère de même sur tous les diviseurs irréductibles de $G(y)$, on peut définir une fois et une fois seulement les racines différentes de $g(y, \xi) = 0$ comme racines des équations

$$d(y, \xi) = 0, \qquad d_1(y, \xi) = 0, \ldots,$$

qui sont de même forme, mais de degré moindre en y, ou comme racines d'équations irréductibles à coefficients entiers.

Faisons remarquer, à ce sujet, que le produit $\prod d(y, \xi_i)$ étendu à toutes les racines de $f(x)$ n'admet que des racines de $H(y) = 0$; ce produit est d'ailleurs un polynome entier en y à coefficients entiers, c'est donc une puissance de $H(y)$.

En particulier, si les racines des équations $d(y, \xi_i) = 0$, $(i = 1, 2, \ldots n)$ sont distinctes, on peut affirmer que l'on a

$$\prod d(y, \xi_i) = H(y).$$

Il n'existe alors aucune décomposition de $d(y, \xi)$ en facteurs qui soient fonctions entières de ξ. Si l'on avait en effet

$$d(y, \xi) = d'(y, \xi) \,.\, d''(y, \xi),$$

cette identité subsisterait pour toutes les racines de $f(x)$ et l'on pourrait en déduire

$$\prod d(y, \xi_i) = \prod d'(y, \xi_i) \,.\, \prod d''(y, \xi),$$

c'est-à-dire que $H(y)$ se décomposerait en facteurs à coefficients entiers.

On dit que ce polynome $d(y, \xi)$ est *irréductible dans le domaine algébrique d'intégrité* $[\xi]$. Ce domaine se compose, comme on l'a dit plus haut, des fonctions entières à coefficients entiers du nombre algébrique entier ξ, et l'on voit que le polynome $d(y, \xi)$ n'admet pas de diviseurs dont les coefficients soient des éléments du domaine.

VI. — Réductibilité dans le domaine algébrique $[\xi]$.

31. Nous avons vu s'introduire, à deux reprises différentes, l'étude de la décomposition d'un polynome entier en y dont les coefficients sont fonctions entières d'un nombre algébrique entier ξ en polynomes possédant les mêmes propriétés. Il convient d'appeler ici l'attention sur l'importance de cette étude, importance qui va résulter de la recherche de son origine naturelle.

Considérons l'équation irréductible $f(x) = 0$ dont ξ est l'une des racines. Nous pouvons supposer qu'on ait commencé l'introduction des nombres algébriques entiers dans le calcul par celle des racines $\xi_1, \xi_2, \ldots, \xi_n$ de cette équation, c'est-à-dire qu'on ait étendu les groupes formés par les nombres entiers pour les deux modes : addition et multiplication, de façon à ce qu'ils renferment les symboles $\xi_1, \xi_2, \ldots, \xi_n$. Les symboles qu'il est alors nécessaire d'introduire avec $\xi_1, \xi_2, \ldots, \xi_n$ sont nécessairement tous ceux qui résultent d'une composition répétée : addition ou multiplication, des symboles $\xi_1, \xi_2, \ldots, \xi_n$ entre eux ou avec les nombres entiers, c'est-à-dire toutes les fonctions entières à coefficients entiers de $\xi_1, \xi_2, \ldots, \xi_n$. On peut dire qu'ils constituent le *domaine algébrique d'intégrité* $[\xi_1, \xi_2, \ldots, \xi_n]$.

Signalons en passant la différence essentielle qui existe, pour nous, entre un domaine *algébrique* d'intégrité $[\xi_1, \xi_2, \ldots, \xi_n]$ et un domaine d'intégrité $[a, b, \ldots, l]$ renfermant seulement des variables indéterminées, domaine qu'on appelle d'habitude *naturel*. Les éléments de ces domaines constituent un groupe, soit par leur addition, soit par leur multiplication, mais alors que la table de structure du groupe formé des fonctions entières de $a, b, \ldots, l$ dérive uniquement des lois *naturelles* de l'addition et de la multiplication, la table de structure du groupe formé de l'ensemble des fonctions entières à coefficients entiers de $\xi_1, \xi_2, \ldots, \xi_n$ nécessite, pour être construite, l'usage des n *relations fondamentales* ajoutées arbitrairement :

$$\begin{gathered}\xi_1 + \xi_2 + \cdots + \xi_n = p_1, \\ \ldots\ldots\ldots\ldots, \\ \ldots\ldots\ldots\ldots, \\ \xi_1\xi_2 \ldots\ldots\ldots\ldots \xi_n = p_n.\end{gathered}$$

L'introduction dans le calcul, des nombres algébriques $\xi_1, \xi_2, \ldots, \xi_n$ change le caractère de certaines équations irréductibles. On voit en effet que des équations, irréductibles dans le domaine des nombres entiers, deviennent réductibles dans le domaine $[\xi_1, \xi_2, \ldots \xi_n]$; en particulier celles qui admettent pour racines des fonctions entières à coefficients entiers de $\xi_1, \xi_2, \ldots, \xi_n$, admettront des diviseurs du premier degré. Si l'on veut, par conséquent, continuer l'introduction des symboles algébriques en se bornant aux *symboles nécessaires*, c'est-à-dire en n'employant de nouveaux noms et de nouveaux signes que pour des symboles qui ne s'expriment pas comme fonctions entières de $\xi_1, \xi_2, \ldots, \xi_n$, il sera *indispensable* de savoir décomposer un polynome irréductible $g(y)$ en facteurs qui soient des fonctions entières de $\xi_1, \xi_2, \ldots, \xi_n$ ou du moins de reconnaître si une telle décomposition existe et de la pousser dans ce cas aussi loin que possible. On ne s'arrêtera donc que lorsqu'on parviendra à des polynomes $d(y, \xi_1, \xi_2, \ldots, \xi_n)$ pour lesquels il n'existera pas de diviseurs entiers en $y, \xi_1, \xi_2, \ldots, \xi_n$ et qu'on appellera polynomes *irréductibles dans le domaine algébrique d'intégrité* $[\xi_1, \xi_2, \ldots, \xi_n]$.

L'étude de la réductibilité dans un domaine algébrique $[\xi_1, \xi_2, \ldots, \xi_n]$ s'offre donc dès le début comme une chose essentielle à approfondir pour que l'on puisse constituer synthétiquement l'ensemble des entiers algébriques, et de plus, à approfondir *avec des moyens déterminés* : on ne doit en effet faire usage que des éléments déjà introduits dans le calcul, c'est-à-dire ceux du domaine $[\xi_1, \xi_2, \ldots, \xi_n]$.

32. Faisons en terminant une observation importante. Nous avons vu qu'on est conduit à introduire simultanément dans le calcul, les n symboles qui vérifient la relation $f(x) = 0$. Il n'est pas indispensable d'opérer ainsi. Par exemple, on peut se proposer, en introduisant dans le calcul les symboles algébriques, d'*en introduire le moins possible à la fois*. Considérons par exemple, l'équation $f(x) = 0$ sur laquelle nous venons de raisonner; nous désignerons par ξ une racine de cette équation, naturellement prise au hasard parmi ses n racines, c'est-à-dire un symbole qui, vérifiant la condition $f(\xi) = 0$, se composera avec lui-même et avec les nombres entiers en suivant les lois de l'addition et de la multiplication des entiers, et nous considérerons l'ensemble des symboles qu'on obtient ainsi, c'est-à-dire *le domaine algébrique d'intégrité* $[\xi]$. Nous

remarquons que le caractère de certaines équations au point de vue de l'existence ou de la non existence des racines a changé complètement ; il existe en effet comme précédemment des équations irréductibles dans le domaine des nombres entiers qui admettent des racines dans le domaine $[\xi]$, d'autres qui sans admettre de racines se décomposent en équations d'ordre inférieur, etc. Il est également indispensable ici, pour continuer l'introduction des symboles algébriques sans en introduire de superflus, de pouvoir fixer la décomposition de tout polynome irréductible à coefficients entiers, dans le nouveau domaine, c'est-à-dire d'étudier la réductibilité dans le domaine algébrique d'intégrité $[\xi]$. Comme précédemment, il est nécessaire de faire cela en n'employant que les éléments déjà introduits dans le calcul, c'est-à-dire les fonctions entières de ξ à coefficients entiers. A l'égard du domaine $[\xi]$ nous ferons remarquer qu'*a priori* il paraît beaucoup plus simple que le domaine $[\xi_1, \xi_2, \ldots, \xi_n]$; pour construire en effet les tables de structure des groupes que constituent ses éléments, il suffira de tenir compte d'*une seule relation fondamentale*, $f(\xi) = 0$. On peut en outre ajouter que tous les éléments du domaine sont distincts, puisque la seule relation rationnelle que vérifie ξ est la relation $f(\xi) = 0$; il n'en est pas toujours de même des éléments du domaine $[\xi_1, \xi_2, \ldots, \xi_n]$, c'est-à-dire des polynomes entiers en $\xi_1, \xi_2, \ldots, \xi_n$ de degré $n - i$ en ξ_i, et nous verrons que c'est là ce qui fait à la fois la difficulté et l'importance de l'étude séparée des diverses équations irréductibles, lorsqu'on introduit simultanément toutes leurs racines, ce qui est indispensable pour les étudier complètement.

CHAPITRE III

LES SYSTÈMES D'ÉQUATIONS

---

33. Désignons par $f(x)$ le polynome irréductible à coefficients entiers

$$x^n - p_1 x^{n-1} + \ldots \pm p_n;$$

nous avons vu dans le chapitre précédent que si des symboles différents $\xi_1, \xi_2, \ldots, \xi_n$, possédant les deux modes de composition des entiers positifs que l'on appelle addition et multiplication, vérifient les n relations

$$f(\xi_i) = 0, \qquad (i = 1, 2, \ldots, n),$$

ces mêmes symboles vérifient également l'identité en x

$$f(x) = (x - \xi_1)(x - \xi_2) \ldots (x - \xi_n)$$

ou encore les n relations

$$S_1 = p_1, \qquad S_2 = p_2, \ldots, S_n = p_n,$$

lorsqu'on désigne par $S_1, S_2, \ldots, S_n$ leurs fonctions symétriques élémentaires. Il est visible que, réciproquement, lorsque des symboles différents $\eta_1, \eta_2, \ldots, \eta_n$, possédant les mêmes modes de composition, vérifient ces dernières relations, l'on pourra écrire l'identité en x

$$f(x) = (x - \eta_1)(x - \eta_2) \ldots (x - \eta_n),$$

et si l'on observe enfin qu'un polynome entier à coefficients entiers ne peut être décomposé en facteurs du premier degré $x - x_n$, où les x_i possèdent les modes de composition indiqués plus haut, que d'une seule manière, on en conclura qu'*à l'ordre de leurs éléments*

près, les deux suites $\xi_1, \xi_2, \ldots, \xi_n$ et $\eta_1, \eta_2, \ldots, \eta_n$ sont identiques. Nous pourrons par conséquent, en faisant abstraction de cet ordre, qui dépend uniquement des notations adoptées, *lesquelles ont été choisies arbitrairement*, regarder les ξ comme assujettis simplement à posséder les deux modes de composition déjà spécifiés et à vérifier les n relations

$$S_1 = p_1, \qquad S_2 = p_2, \qquad \ldots \qquad S_n = p_n.$$

C'est de là que nous partirons pour établir que le calcul des symboles ξ est déterminé d'une manière unique et ne renferme point de contradiction. On a déjà fait observer qu'il est indispensable pour cet objet de savoir former toutes les conséquences des relations de définition ; ajoutons ici qu'il n'y a évidemment lieu pour nous de considérer que celles de ces conséquences qui se déduisent des relations données par l'application des deux seuls modes de composition des ξ que nous avons définis. Nous sommes ainsi amenés à rechercher toutes les relations entières en $\xi_1, \xi_2, \ldots, \xi_n$ à coefficients entiers qui se peuvent conclure des relations

$$S_1 = p_1, \qquad S_2 = p_2, \qquad \ldots \qquad S_n = p_n.$$

Nous étudierons dans ce chapitre le problème plus général qui consiste à rechercher toutes les relations entières en $x_1, x_2, \ldots, x_n$ à coefficients entiers qui résultent *nécessairement* de p relations données :

$$\begin{aligned} F_1(x_1, x_2, \ldots, x_n) &= 0, \\ F_2(x_1, x_2, \ldots, x_n) &= 0, \\ \cdots\cdots\cdots\cdots \\ F_p(x_1, x_2, \ldots, x_n) &= 0, \end{aligned}$$

dans lesquelles les F sont des polynomes à coefficients entiers et les x des symboles qui se composent, entre eux et avec les nombres entiers, par addition et multiplication en suivant les lois de composition des nombres entiers. Il nous semble inutile de rappeler qu'il en résulte que les polynomes entiers en $x_1, x_2, \ldots, x_n$ à coefficients entiers se composent alors entre eux de la même manière.

Enfin, parmi les divers systèmes de relations que l'on peut ainsi former, nous insisterons plus particulièrement sur ceux qui *déterminent* les symboles $x_1, x_2, \ldots, x_n$. Nous voulons dire par là que les relations données n'étant point contradictoires, aucun des sym-

boles $x_1, x_2, \ldots, x_n$ ne peut être choisi d'une façon arbitraire dans un ensemble de symboles connus, par exemple parmi les nombres entiers ; nous donnerons à ces systèmes le nom de *systèmes d'équations à solutions déterminées.*

I. — Les équations linéaires.

34. Examinons d'abord un cas très simple, dont la solution sera cependant fréquemment appliquée dans la suite ; ce cas est celui dans lequel *tous les polynomes* $F_1, F_2, \ldots, F_p$ *sont du premier degré par rapport à chacun des symboles* $x_1, x_2, \ldots, x_n$ *et aussi par rapport à leur ensemble;* on dit qu'ils sont *linéaires* en $x_1, x_2, \ldots, x_n$.

Le système d'équations donné a par conséquent la forme

$$
(\mathrm{I}) \quad \left\{
\begin{array}{l}
F_1 = a_{1,1}x_1 + a_{1,2}x_2 + \ldots + a_{1,n}x_n + b_1 = 0, \\
F_2 = a_{2,1}x_1 + a_{2,2}x_2 + \cdots + a_{2,n}x_n + b_2 = 0, \\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
F_p = a_{p,1}x_1 + a_{p,2}x_2 + \ldots + a_{p,n}x_n + b_p = 0.
\end{array}
\right.
$$

Nous y supposerons en premier lieu $p = n$, c'est-à-dire *le nombre des relations égal au nombre des symboles* x *qui y figurent.*

Considérons un nouveau symbole z lié aux x par la relation

$$z = u_1x_1 + u_2x_2 + \cdots + u_nx_n\,,$$

dans laquelle les u sont des nombres entiers dont on ne fixe pas d'abord la détermination, mais que l'on ne supposera jamais nuls simultanément, de sorte qu'il n'y a réellement que $n-1$ des u qui sont indéterminés ; on peut regarder l'ensemble des relations données et de la nouvelle relation

$$F_{n+1} = u_1x_1 + \cdots + u_nx_n - z = 0$$

comme un système de $(n+1)$ relations entre les $(n+1)$ symboles $x_1, x_2, \ldots, x_n$ et z ; c'est sur ce système que nous allons raisonner.

Si nous supposons connue la théorie des déterminants, ce qui est légitime puisque cette théorie s'établit indépendamment de nos

considérations (*), nous observons que ces $(n+1)$ relations expriment simplement que les éléments de la dernière colonne du déterminant D :

$$D = \begin{vmatrix} a_{1,1} & a_{1,2} & \ldots & a_{1,n} & b_1 \\ a_{2,1} & a_{2,2} & \ldots & a_{2,n} & b_2 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{n,1} & a_{n,2} & \ldots & a_{n,n} & b_n \\ u_1 & u_2 & \ldots & u_n & -z \end{vmatrix}$$

sont une même fonction linéaire et homogène des éléments correspondants des n premières. Le déterminant D est donc égal à zéro, et en le développant suivant les éléments de la dernière ligne on a

$$\Delta z = \Delta_1 u_1 + \Delta_2 u_2 + \cdots + \Delta_n u_n,$$

$\Delta, \Delta_1, \ldots, \Delta_n$ étant des déterminants qu'il est facile de former.

Le déterminant Δ est un nombre entier déterminé, *supposons-le différent de zéro* ; il résultera de là que quelles que soient les déterminations entières que l'on donne aux u, z sera un nombre rationnel déterminé. Il suffit en outre de remarquer qu'en remplaçant u_i par $u_i + h$ on doit obtenir une identité en h pour déduire de cette même relation en z, les n relations

$$\text{(II)} \qquad \Delta x_1 = \Delta_1, \qquad \Delta x_2 = \Delta_2, \qquad \ldots, \qquad \Delta x_n = \Delta_n,$$

qui expriment que les x sont également des nombres rationnels déterminés.

Considérons ces n relations (II) qui sont, d'après notre raisonnement, des conséquences nécessaires des relations données ; il est facile de voir qu'elles sont simplement des combinaisons linéaires à coefficients entiers de ces dernières. On a en effet identiquement

$$\Delta x_i - \Delta_i = A_{1,i}F_1 + A_{2,i}F_2 + \cdots + A_{n,i}F_n,$$

en désignant par $A_{1,i}, A_{2,i}, \ldots, A_{n,i}$, les coefficients des éléments de la colonne de rang i dans le développement de Δ

$$\Delta = a_{1,i}A_{1,i} + \cdots + a_{n,i}A_{n,i}.$$

(*) L'emploi des déterminants n'est d'ailleurs nullement indispensable ici ; nous l'adoptons uniquement parce qu'il permet d'arriver d'une manière commode à des résultats mis sous une forme élégante.

Nous allons montrer qu'à un facteur près égal à Δ, la réciproque a lieu et par conséquent que les relations données entre les x sont également des conséquences nécessaires des relations (II).

Si l'on considère, en effet, les égalités

$$a_{k,1}\Delta_1 + a_{k,2}\Delta_2 + \cdots + a_{k,n}\Delta_n + b_k\Delta = 0$$
$$(k = 1, 2, \ldots n),$$

qui expriment une propriété bien connue du déterminant D, elles permettent d'écrire les identités en $x_1, x_2, \ldots, x_n$

$$\Delta F_k = a_{k,1}(\Delta x_1 - \Delta_1) + \cdots + a_{k,n}(\Delta x_n - \Delta_n)$$
$$(k = 1, 2, \ldots n),$$

et, comme nous supposons Δ différent de zéro, on pourra déduire des relations (II) les relations données

$$F_k = 0 \qquad (k = 1, 2, \ldots, n).$$

Les systèmes (I) et (II), dans le cas où Δ est différent de zéro, *conduisent par suite aux mêmes conséquences relativement à* $x_1, x_2, \ldots x_n$; on dit de deux systèmes qui possèdent cette propriété qu'ils sont *équivalents*.

35. La connaissance du cas où Δ est égal à zéro résulte de l'étude du cas général où *le nombre* p *des équations n'est pas nécessairement égal au nombre* n *des symboles* $x_1, x_2, \ldots x_n$. Nous supposons bien entendu pour cette étude que tous les coefficients $a_{i,k}(i = 1, 2, \ldots, p, \; k = 1, 2, \ldots, n)$ ne sont pas nuls, sans quoi les symboles $x_1, \ldots, x_n$ disparaîtraient des équations données. On peut alors affirmer que *tous les déterminants qu'on peut former avec les coefficients de* r *symboles pris dans* r *équations quelconques, ne sont pas nuls quel que soit* r, puisque pour $r = 1$ ces déterminants sont les coefficients $a_{i,k}$. Il existe donc un nombre entier positif r, au plus égal au plus petit des nombres n et p, tel que tous les déterminants d'ordre supérieur à r, formés comme il vient d'être dit, sont nuls, l'un au moins des déterminants d'ordre r étant différent de zéro. Nous désignerons par Δ ce déterminant d'ordre r et nous l'appellerons *déterminant principal*.

Considérons les r équations qui ont conduit à ce déterminant Δ; nous pouvons toujours supposer, en changeant les notations, que les r symboles dont les coefficients figurent dans Δ sont précisé-

ment $x_1, x_2, \ldots, x_r$. Il est alors clair que l'on peut remplacer ces r équations par le système *équivalent*

$$\text{(III)} \qquad \Delta x_i = \Delta_{i,r+1} x_{r+1} + \cdots + \Delta_{i,n} x_n + \Delta_i$$
$$(i = 1, 2, \ldots, r),$$

dans lesquel les $\Delta_{i,n+k}$ sont des déterminants dont la composition est immédiate. Envisageons maintenant les $p - r$ équations qui restent

$$F_\alpha = a_{\alpha,1} x_1 + a_{\alpha,2} x_2 + \cdots + a_{\alpha,n} x_n + b_\alpha = 0$$
$$(\alpha = r + 1, \ldots, p);$$

il résulte de l'expression obtenue plus haut pour

$$u_1 x_1 + u_2 x_2 + \ldots + u_n x_n,$$

que l'on peut écrire la relation

$$\Delta F_\alpha = C_\alpha,$$

en désignant par C_α le déterminant

$$\left| \begin{array}{c|c} & a_{1,r+1}\, x_{r+1} + \cdots + a_{1,n}\, x_n + b_1 \\ \Delta & \ldots\ldots\ldots\ldots\ldots \\ & \ldots\ldots\ldots\ldots\ldots \\ & a_{r,r+1}\, x_{r+1} + \cdots + a_{r,n}\, x_n + b_n \\ \hline a_{\alpha,1} \;\ldots,\; a_{\alpha,r} & a_{\alpha,r+1}\, x_{r+1} + \cdots + a_{\alpha,n}\, x_n + b_\alpha \end{array} \right|$$

obtenu en bordant Δ d'une ligne et d'une colonne, déterminant qui se réduit manifestement à

$$\left| \begin{array}{c|c} & b_1 \\ \Delta & \vdots \\ & b_r \\ \hline a_{\alpha,1} \;\ldots\; a_{\alpha,r} & b_\alpha \end{array} \right|$$

d'après les hypothèses faites pour définir Δ. Ce résultat pouvait d'ailleurs s'obtenir immédiatement en tenant compte des équations (III).

Les déterminants C_α que l'on vient de former sont appelés *déterminants caractéristiques*. On voit que si tous ces déterminants sont nuls les $(p - r)$ équations $F_\alpha = 0$ sont des conséquences nécessaires des équations (III); *le système des équations données est donc équivalent au système* (III) *formé seulement de r équations*.

Si, au contraire, les C_α ne sont pas tous nuls, il est impossible

que les relations (III) et les relations $F_\alpha = 0$ aient lieu simultanément; *les équations données sont donc contradictoires avec les conditions imposées aux symboles $x_1, x_2, \ldots, x_n$;* on dit aussi quelquefois qu'elles sont *incompatibles.*

36. Il est bien clair que dans le cas où tous les C_α sont nuls, si nous choisissons pour $x_{r+1}, \ldots, x_n$ des nombres rationnels arbitraires, les r équations (III) expriment que $x_1, x_2, \ldots, x_n$ sont des nombres rationnels bien déterminés. On obtient d'ailleurs ainsi tous les systèmes de nombres rationnels qui vérifient les équations (III).

Nous dirons, pour mettre ce fait en évidence, que le système (III) présente une *indétermination d'ordre* $(n - r)$ ou encore que ses solutions sont $(n - r)$ fois indéterminées, en appelant *solution* du système tout ensemble de nombres rationnels qui, mis respectivement à la place de $x_1, x_2, \ldots, x_n$, transforment les relations (III) en identités.

Nous ferons également observer ici, dans le cas particulier de n équations entre n symboles x_i pour lesquelles les b sont tous nuls, c'est-à-dire dans le cas de n équations *homogènes*, que lorsque le déterminant des $a_{i,k}$ n'est pas nul, les nombres rationnels qui sont définis d'une manière unique par ces équations sont tous nuls et que lorsque le déterminant des $a_{i,k}$ est nul, il existe certainement d'autres solutions. On conclut de là la réciproque d'une proposition bien connue de la théorie des déterminants, réciproque qu'on peut énoncer ainsi : *si un déterminant est nul, les éléments de chacune de ses lignes vérifient une même relation linéaire et homogène, dont les coefficients ne sont pas tous nuls. La même proposition a lieu pour les colonnes.* Nous aurons, plus loin, l'occasion d'utiliser cette remarque.

II. — Résultant de deux polynomes. — Discriminant.

37. Avant d'aborder des cas plus complexes, il est commode de résoudre une question dont la solution sera utilisée dans leur étude. C'est ce que nous nous proposons de faire maintenant, en insistant même un peu plus qu'il ne le serait strictement nécessaire pour les

applications ultérieures, à cause de l'intérêt que présente la question en elle-même.

On considère deux polynomes entiers en x, *de degrés déterminés* m *et* p :

$$f(x) = x^m + a_1x^{m-1} + \cdots + a_m,$$
$$g(x) = x^p + b_1x^{p-1} + \cdots + b_p,$$

ayant comme coefficients des entiers dont on ne fixe pas d'abord la détermination ; on demande de former des relations nécessaires et suffisantes que devront vérifier ces entiers pour que les polynomes aient un plus grand commun diviseur de degré déterminé, q.

Si les polynomes $f(x)$ et $g(x)$ ont un plus grand commun diviseur $D(x)$, de degré q, on peut écrire les identités en x :

$$f(x) = D(x).f_1(x),$$
$$g(x) = -D(x).g_1(x),$$

dans lesquelles $f_1(x)$ et $g_1(x)$ sont des polynomes entiers en x, à coefficients entiers, de degrés respectivement $m-q$ et $p-q$ et dont on peut supposer les premiers coefficients égaux l'un à $+1$ l'autre à -1. On déduit de là la nouvelle identité

$$f(x).g_1(x) + f_1(x).g(x) = 0.$$

Inversement, si $f_1(x)$ et $g_1(x)$ sont des polynomes de degrés $m-q$ et $p-q$ vérifiant l'identité

$$f(x).g_1(x) + f_1(x).g(x) = 0,$$

il existe entre $f(x)$ et $g(x)$ un plus grand diviseur commun de degré *au moins égal à* q. En effet, dans le cas où $f_1(x)$ et $g_1(x)$ sont premiers entre eux, l'identité précédente montre que $g_1(x)$ est un diviseur de $g(x)$, et si l'on écrit

$$g(x) = -g_1(x).D(x),$$

$D(x)$ étant de degré q, il en résulte $f(x) = -f_1(x).D(x)$, ce qui établit la proposition. Si, au contraire, $f_1(x)$ et $g_1(x)$ ont un plus grand diviseur commun de degré r, on a, en désignant par $f_2(x)$ et $g_2(x)$ leurs quotients par ce diviseur, la nouvelle identité

$$f(x).g_2(x) + f_2(x).g(x) = 0,$$

qui exprime que $f(x)$ et $g(x)$ ont un plus grand commun diviseur de degré $q+r$.

Nous sommes ainsi ramenés à *chercher des conditions nécessaires*

et suffisantes pour qu'il existe des polynomes en x, de degrés respectivement $m-q$ et $p-q$, vérifiant l'identité

$$f(x).g_1(x)+f_1(x).g(x)=0.$$

Posons, d'une manière générale,

$$f_1(x)=\alpha_1x^{m-1}+\alpha_2x^{m-2}+\cdots+\alpha_m,$$
$$g_1(x)=\beta_1x^{p-1}+\beta_2x^{p-2}+\cdots+\beta_p;$$

on aura l'identité en x

$$f(x).g_1(x)+f_1(x).g(x)=\beta_1\mathrm{F}_1+\beta_2\mathrm{F}_2+\cdots+\beta_p\mathrm{F}_p+\alpha_m\mathrm{G}_m+\cdots+\alpha_1\mathrm{G}_1,$$

dans laquelle F_i et G_k désignent respectivement les polynomes

$$x^{p-i}f(x) \qquad \text{et} \qquad x^{m-k}g(x).$$

Considérons maintenant le déterminant R, d'ordre $m+p$, formé avec les coefficients des $m+p$ polynomes $\mathrm{F}_1, \ldots, \mathrm{F}_p, \mathrm{G}_m, \ldots, \mathrm{G}_1$, dont le degré en x est au plus égal à $m+p-1$; on a

$$\mathrm{R}=\begin{vmatrix}
1 & a_1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & a_{m-1} & a_m & 0 & \cdot & \cdot & \cdot & 0\\
0 & 1 & a_1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & a_m & 0 & \cdot & \cdot & 0\\
0 & 0 & 1 & a_1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & a_m & 0 & \cdot & 0\\
0 & \cdot & 0 & 1 & a_1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & a_m & 0 & 0\\
0 & \cdot & \cdot & 0 & 1 & a_1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & a_m & 0\\
0 & & \cdot & \cdot & 0 & 1 & a_1 & \cdot & \cdot & a_{m-p} & \cdot & \cdot & \cdot & \cdot & \cdot & a_m\\
0 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0 & 1 & b_1 & \cdot & \cdot & \cdot & \cdot & b_p\\
0 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0 & 1 & b_1 & \cdot & \cdot & \cdot & \cdot & b_p & 0\\
0 & \cdot & \cdot & \cdot & \cdot & \cdot & 0 & 1 & b_1 & \cdot & \cdot & \cdot & \cdot & b_p & 0 & 0\\
0 & \cdot & \cdot & \cdot & \cdot & 0 & 1 & b_1 & \cdot & \cdot & \cdot & \cdot & b_p & 0 & \cdot & 0\\
0 & \cdot & \cdot & \cdot & 0 & 1 & b_1 & \cdot & \cdot & \cdot & \cdot & b_p & 0 & \cdot & \cdot & 0\\
0 & \cdot & \cdot & 0 & 1 & b_1 & \cdot & \cdot & \cdot & \cdot & b_p & 0 & \cdot & \cdot & \cdot & 0\\
0 & \cdot & 0 & 1 & b_1 & \cdot & \cdot & \cdot & \cdot & b_p & 0 & \cdot & \cdot & \cdot & \cdot & 0\\
0 & 0 & 1 & b_1 & \cdot & \cdot & \cdot & \cdot & b_p & 0 & \cdot & \cdot & \cdot & \cdot & \cdot & 0\\
0 & 1 & b_1 & \cdot & \cdot & \cdot & \cdot & b_p & 0 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0\\
1 & b_1 & \cdot & \cdot & \cdot & b_{p-1} & b_p & 0 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0
\end{vmatrix}$$

Nous observons que l'identité en x

$$\beta_1\mathrm{F}_1+\cdots+\beta_p\mathrm{F}_p+\alpha_m\mathrm{G}_m+\cdots+\alpha_1\mathrm{G}_1=0$$

exprime simplement qu'il existe entre les éléments $y_1, y_2, \ldots, y_{p+m}$ de chaque colonne du déterminant R, la relation linéaire et homogène

$$\beta_1 y_1 + \cdots + \beta_p y_p + \alpha_m y_{p+1} + \cdots + \alpha_1 y_{p+m} = 0,$$

et par suite que ce déterminant R est nul. Réciproquement, lorsque R est nul, il existe entre les éléments de chaque colonne de R une même relation linéaire et homogène dont les coefficients ne sont pas tous nuls ; on peut donc écrire l'identité en x

$$\beta_1 F_1 + \cdots + \beta_p F_p + \alpha_m G_m + \cdots + \alpha_1 G_1 = 0,$$

en désignant par $\beta_1, \ldots, \beta_p, \alpha_m, \ldots, \alpha_1$ les coefficients de cette relation. Faisons remarquer qu'il résulte de ce que les coefficients des plus hautes puissances de x, dans les F et les G, sont toujours égaux à l'unité, que si β_i est le premier des β qui soit différent de zéro, α_i, qui est égal à $-\beta_i$, est nécessairement différent de zéro et c'est le premier des α qui n'est pas nul. L'identité écrite exprime dans ce cas que le plus grand commun diviseur de $f(x)$ et $g(x)$ est au moins de degré i.

Nous pouvons conclure de ce qui précède que *la relation* $R = 0$ *est nécessaire et suffisante pour que les polynomes* $f(x)$ *et* $g(x)$ *aient un diviseur commun.*

38. Proposons-nous de chercher des conditions nécessaires et suffisantes pour que le diviseur commun soit au moins du second degré, c'est-à-dire pour qu'il existe une identité en x :

$$\beta_2 F_2 + \cdots + \beta_p F_p + \alpha_m G_m + \cdots + \alpha_2 G_2 = 0.$$

Une identité de cette forme, lorsqu'elle existe, exprime *en particulier* que les éléments $y_2, y_3, \ldots, y_{p+m-1}$ de chaque colonne du déterminant R_1, qu'on obtient en supprimant dans R les lignes et les colonnes extrêmes, sont liés par la relation

$$\beta_2 y_2 + \cdots + \beta_p y_p + \alpha_m y_{p+1} + \cdots + \alpha_2 y_{p+m-1} = 0,$$

et par suite que le déterminant R_1 est nul.

Inversement, si l'on a $R_1 = 0$, il existe des coefficients non tous nuls, $\beta_2, \ldots, \beta_p, \alpha_m, \ldots, \alpha_2$, tels que l'on ait pour chaque colonne de R_1 la relation

$$\beta_2 y_2 + \cdots + \beta_p y_p + \alpha_m y_{p+1} + \cdots + \alpha_2 y_{p+m-1} = 0.$$

Formons avec ces coefficients l'expression

$$\beta_2 F_2 + \cdots + \beta_p F_p + \alpha_m G_m + \cdots + \alpha_2 G_2 ;$$

elle se réduira visiblement à la combinaison indépendante de x :

$$\beta_p a_m + \alpha_m b_p.$$

Mais si nous supposons que l'on a également $R = 0$, c'est-à-dire qu'il existe un diviseur commun à $f(x)$ et à $g(x)$, cette expression sera nécessairement égale à zéro. On aura donc l'identité

$$\beta_2 F_2 + \ldots + \beta_p F_p + \alpha_m G_m + \ldots + \alpha_2 G_2 = 0,$$

et par suite $f(x)$ et $g(x)$ admettront un diviseur commun qui sera au moins du second degré.

Les relations $R = 0$, $R_1 = 0$ *donnent ainsi des conditions nécessaires et suffisantes pour l'existence d'un diviseur commun à* $f(x)$ *et à* $g(x)$ *dont le degré soit au moins égal à* 2.

La proposition peut d'ailleurs s'étendre facilement ; il suffit de la supposer démontrée lorsque le diviseur commun est de degré au moins égal à q, pour qu'on puisse l'établir, en appliquant le raisonnement précédent, dans le cas où ce diviseur commun est au moins de degré $q+1$. Si l'on désigne par R_i le déterminant d'ordre $m+p-2i$ que l'on obtient en supprimant dans R, les $2i$ lignes et les $2i$ colonnes extrêmes (les i premières et les i dernières), on peut donc dire que *les relations*

$$R = 0, \qquad R_1 = 0, \ \ldots \ R_{q-1} = 0$$

sont nécessaires et suffisantes pour que les polynomes $f(x)$ *et* $g(x)$ *aient un diviseur commun de degré au moins égal à* q.

Il est aisé de donner, lorsqu'on fixe son degré, l'expression du plus grand commun diviseur des deux polynomes $f(x)$ et $g(x)$. Considérons, en effet, la suite des déterminants $R_1, R_2, \ldots, R_q$ dont chacun se déduit du précédent par suppression des lignes et des colonnes extrêmes ; nous désignerons par

$$B_{i+1,i}, \ldots, \quad B_{p,i}, \quad A_{m,i}, \ldots, \quad A_{i+1,i}$$

les coefficients des éléments de la dernière colonne de R_i dans le développement de ce déterminant.

On a évidemment les identités en x :

$$B_{2,1}F_2 + \ldots + B_{p,1}F_p + A_{m,1}G_m + \ldots + A_{2,1}G_2 = R_1 x + S_{1,1},$$
$$B_{3,2}F_3 + \ldots + B_{p,2}F_p + A_{m,2}G_m + \ldots + A_{3,2}G_3 = R_2 x^2 + S_{1,2}x + S_{2,2},$$

. . . .

$$B_{i+1,i}F_{i+1} + \ldots B_{p,i}F_p + A_{m,i}G_m + \ldots + A_{i+1,i}G_i = R_i x^i + S_{1,i}x^{i-1} + \ldots + S_{i,i},$$

. . . .

dont le nombre est le plus petit des entiers m et p. Les coefficients $S_{k,i}$ qui figurent dans les seconds membres, sont des déterminants qu'on déduit de R_i en y remplaçant simplement les éléments de la dernière colonne par les éléments correspondants de la colonne de R, dont le rang surpasse de k celui de cette dernière colonne de R_i.

Ces identités montrent immédiatement que si l'on a

$$R = 0, \qquad R_1 = 0, \qquad \ldots, \qquad R_{q-1} = 0,$$

mais non $R_q = 0$, le degré du diviseur commun qui est au moins égal à q ne peut surpasser q. *Il existe donc dans ce cas un plus grand diviseur commun de degré q, qui, à un facteur près indépendant de x, est nécessairement le polynome*

$$R_q x^q + S_{1,q} x^{q-1} + \cdots + S_{q,q}.$$

39. Le déterminant R, que nous avons appris à former, et qui, lorsqu'on l'égale à zéro, donne la condition nécessaire et suffisante de l'existence d'un diviseur commun à $f(x)$ et à $g(x)$, est appelé le *résultant* de ces deux polynomes. Nous nous bornerons à en signaler maintenant deux propriétés importantes.

La première est exprimée par l'identité

$$B_1F_1 + \cdots + B_pF_p + A_mG_m + \cdots + A_1G_1 = R,$$

dans laquelle nous avons désigné par $B_1, \ldots, B_p, A_m, \ldots, A_1$ les coefficients des éléments de la dernière colonne du déterminant R dans le développement de ce déterminant ; on l'énonce en disant que *le résultant* R *est une combinaison linéaire des polynomes*

$$f(x) \text{ et } g(x).$$

La seconde, d'une nature toute différente, est relative à la constitution de R considéré comme polynome en $a_1, a_2, \ldots, a_m, b_1, b_2, \ldots, b_p$: *Lorsqu'on remplace dans* R *les symboles a_i et b_k respectivement par $a_i\lambda^i$ et $b_k\lambda^k$ pour toutes les valeurs de i et k, on obtient un monome en λ de degré mp.*

Envisageons en effet le déterminant par lequel nous avons exprimé ce résultant ; il est clair qu'il suffit de multiplier respectivement par $\lambda, \lambda^2, \ldots, \lambda^p, \lambda^m, \lambda^{m-1}, \ldots, \lambda$ les éléments des lignes de ce déterminant prises dans leur ordre naturel, pour que la colonne de rang r soit uniquement formée d'éléments de degré r par rapport à λ.

On obtient donc ainsi un monome en λ de degré égal à la somme $1+2+\cdots+(m+p)$, c'est-à-dire de degré $\frac{(m+p)(m+p-1)}{2}$, et si l'on remarque qu'on a multiplié R par une puissance de λ d'ordre égal à $\frac{p(p-1)}{2}+\frac{m(m-1)}{2}$, l'on pourra en conclure que R était un monome en λ de degré égal à

$$\frac{(m+p)(m+p-1)}{2}-\frac{p(p-1)}{2}-\frac{m(m-1)}{2},$$

c'est-à-dire de degré égal à mp. C'est précisément la proposition annoncée.

Une autre propriété du résultant se laisse facilement déduire de là. Nous supposerons pour l'établir que les polynomes $f(x)$ et $g(x)$ sont décomposables en facteurs du premier degré ; nous voulons dire par là qu'on a les deux identités en x

$$f(x)=(x-y_1)(x-y_2)\ldots(x-y_m),$$

$$g(x)=(x-z_1)(x-z_2)\ldots(x-z_p),$$

dans lesquelles les y et les z désignent des entiers dont on ne fixe pas la détermination. Les a et les b sont alors, au signe près, les fonctions symétriques élémentaires des y et des z, et si l'on remarque que a_i et b_i sont précisément de degré i par rapport à l'ensemble des lettres y et z, on peut en conclure, en se reportant à la démonstration précédente, que le résultant R est un polynome entier par rapport aux y et aux z, dont les coefficients sont entiers et le degré par rapport à l'ensemble de ces lettres égal à mp. Il est aisé de donner l'expression de ce polynome. Si nous observons, en effet, que lorsqu'on remplace y_i par z_k, quels que soient d'ailleurs i et k, les deux polynomes $f(x)$ et $g(x)$ ont le diviseur commun $x-z_k$, on voit que le polynome R est nécessairement divisible par y_i-z_k. Il ne peut donc différer du produit $\prod_{i=1}^{i=m}\prod_{k=1}^{k=p}(y_i-z_k)$ que par un facteur indépendant des y et des z, et l'on s'assure immédiatement par la considération du terme a_m^p ou du terme b_p^m que ce facteur est, au signe près, égal à l'unité.

Nous pouvons donc écrire en faisant abstraction de ce signe

$$R = \prod_{i=1}^{i=m} g(y_i) \qquad \text{ou bien} \qquad R = (-1)^{mp} \prod_{k=1}^{k=p} f(z_k) ;$$

c'est en ces identités que consiste la propriété annoncée.

Passons à l'examen d'une forme particulière du résultant que l'on obtient dans le cas où l'un des deux polynomes $f(x)$ et $g(x)$ est le dérivé de l'autre. Soit par exemple

$$f(x) = x^m + a_1 x^{m-1} + \dots + a_m,$$

$$g(x) = f'(x) = mx^{m-1} + (m-1)a_1 x^{m-1} + \cdots + a_{m-1} ;$$

le résultant des polynomes $f(x)$ et $f'(x)$ est, au facteur m^m près, un polynome entier en $a_1, a_2, \dots, a_m$ à coefficients entiers dont tous les termes sont en λ de degré égal à $m(m-1)$, lorsqu'on y remplace a_i par $a_i\lambda^i$; on le nomme *discriminant* du polynome $f(x)$ et on le désigne habituellement par Δ_f. Il résulte immédiatement de la définition du résultant que la relation $\Delta_f = 0$ exprime la condition nécessaire et suffisante pour qu'il existe un diviseur commun à $f(x)$ et à $f'(x)$ et par conséquent aussi pour que le polynome $f(x)$ possède des diviseurs multiples. Nous savons donc décider, par le seul examen du discriminant, c'est-à-dire sans rechercher le plus grand commun diviseur à $f(x)$ et $f'(x)$, si tous les diviseurs irréductibles de $f(x)$ sont ou non distincts.

Le discriminant du polynome $f(x)$ prend également une forme particulièrement simple et que nous devons signaler, lorsque ce polynome est un produit de facteurs du premier degré. Supposons en effet que l'on ait l'identité en x :

$$f(x) = (x - x_1)(x - x_2) \dots (x - x_m),$$

dans laquelle $x_1, x_2, \dots, x_m$ désignent des entiers indéterminés. Une propriété du résultant, que nous venons d'établir, nous permet d'écrire

$$\Delta_f = \prod_{i=1}^{i=m} f'(x_i),$$

et si nous observons que l'on a

$$f'(x_i) = (x_i - x_1) \dots (x_i - x_{i-1})(x_i - x_{i+1}) \dots (x_i - x_m),$$

nous en conclurons l'identité

$$\Delta_f = \prod_{i=1}^{i=m} \prod_{k=1}^{k=m} (x_i - x_k).$$

L'expression du discriminant ainsi obtenue peut encore être simplifiée en associant les facteurs $x_i - x_k$ et $x_k - x_i$, qui ne diffèrent que par le signe, et nous parvenons ainsi à l'identité

$$\Delta_f = (-1)^{\frac{m(m-1)}{2}} \left[\prod_{i=1}^{i=m} \prod_{k=i}^{k=m} (x_i - x_k) \right]^2,$$

à laquelle nous nous arrêterons. Elle nous montre que le discriminant est à la fois une fonction symétrique entière à coefficients entiers des lettres $x_1, x_2, \ldots, x_n$ et *le carré d'une fonction entière à coefficients entiers de ces mêmes lettres* (*).

40. Il convient, avant d'abandonner la question, d'appeler l'attention sur la signification des résultats acquis dans la recherche des conditions de l'existence d'un diviseur commun à $f(x)$ et à $g(x)$, de degré déterminé, au point de vue même où nous nous sommes placés au début de ce chapitre.

Ce problème nous a en effet conduits à un système de relations :

$$\begin{cases} R = 0, \\ R_1 x + S_{1,1} = 0, \\ R_2 x^2 + S_{1,2} x + S_{2,2} = 0, \\ \ldots\ldots\ldots\ldots \end{cases}$$

qui sont toutes des conséquences nécessaires des relations

$$f(x) = 0, \qquad g(x) = 0,$$

et si nous observons que nous n'avons fait usage pour l'obtenir que des propriétés de deux modes de composition des coefficients $a_1, \ldots, a_m, b_1, \ldots, b_p$ entre eux et avec les entiers positifs, nous pouvons ajouter que *les résultats acquis sont démontrés sous la seule condition que l'on conserve ces deux modes de composition*. C'est là une remarque dont nous aurons bientôt à nous servir.

(*) Il n'est pas inutile d'observer que cette proposition, ainsi d'ailleurs que la proposition analogue établie à l'égard du résultant dans un cas particulier, sera démontrée pour tous les polynomes dès qu'on aura établi la possibilité logique de définir les nombres algébriques ainsi que nous l'avons fait.

Le système que nous venons d'écrire possède en outre des propriétés remarquables qu'il serait intéressant d'approfondir. Nous nous bornerons à signaler la suivante, dont la démonstration est immédiate dès qu'on a établi que *le résultant* R *considéré comme polynome en* $a_1, a_2, \ldots, a_m, b_1, b_2, \ldots, b_p$ *est irréductible :* lorsqu'on suppose R_1 différent de zéro, les deux premières relations :

$$\begin{cases} R = 0, \\ R_1 x + S_{1,1} = 0, \end{cases}$$

forment, vis-à-vis des symboles $a_1, a_2, \ldots, a_m, b_1, b_2, \ldots, b_p$ et x, un système équivalent au système des deux relations

$$f(x) = 0, \qquad g(x) = 0.$$

III. — Systèmes d'équations en x et en y.

41. Nous allons maintenant aborder l'étude des systèmes d'équations renfermant deux symboles x et y et pour plus de netteté nous commencerons par le cas où *le nombre des équations est précisément égal à deux*. Il s'agit par conséquent de rechercher toutes les relations entières en x et en y à coefficients entiers qui sont des conséquences nécessaires des deux relations

$$\text{(I)} \qquad \begin{cases} F(x, y) = 0, \\ G(x, y) = 0. \end{cases}$$

Remarquons immédiatement que si l'on a identiquement

$$F(x, y) = F_1(x, y).F_2(x, y),$$

F_1 et F_2 désignant également des polynomes à coefficients entiers, qui renferment ou non les deux symboles x et y, les conséquences nécessaires des relations (I) sont ou bien des conséquences nécessaires des relations

$$\text{(II)} \qquad \begin{cases} F_1(x, y) = 0, \\ G(x, y) = 0, \end{cases}$$

ou bien des conséquences nécessaires des relations

$$\text{(III)} \qquad \begin{cases} F_2(x, y) = 0, \\ G(x, y) = 0. \end{cases}$$

Réciproquement, les relations (II) ou les relations (III) entraî-

nent nécessairement les relations (I), en sorte que le système (I) est *équivalent*, dans le sens donné plus haut à ce terme, à l'ensemble des systèmes (II) et (III). *On peut donc se borner à considérer des systèmes de la forme* (I) *dans lesquels* $F(x, y)$ *et* $G(x, y)$ *seront des polynomes irréductibles ;* c'est ce que nous ferons effectivement.

Supposons par conséquent $F(x, y)$ et $G(x, y)$ irréductibles et *différents*, de telle sorte que le système (I) renferme bien deux équations ; nous désignerons par λ le degré maximum de F par rapport à l'ensemble des lettres x et y (ce qu'on appelle quelquefois la *dimension maximum* de F) et par μ le nombre analogue relatif à G.

Nous allons, en suivant une méthode déjà employée pour les équations linéaires, rechercher les propriétés du symbole z, lié à x et à y par la relation $z = ux + vy$, relation dans laquelle u et v représentent des nombres entiers dont nous ne fixons pas la détermination et que nous ne ferons jamais nuls simultanément.

Remplaçons, à cet effet, dans les relations

(I) $$F(x, y) = 0, \qquad G(x, y) = 0,$$

multipliées respectivement par v^λ et par v^μ, le produit vy par la différence $z - ux$; nous obtiendrons les nouvelles relations

$$F_1(x, z, u, v) = 0,$$
$$G_1(x, z, u, v) = 0,$$

qui, lorsque v est différent de zéro, sont des conséquences nécessaires des relations données. On observe d'ailleurs que F_1 et G_1 sont homogènes et de dimensions respectivement λ et μ par rapport à u, v et z, et que ces deux polynomes renferment effectivement x, l'un à la puissance λ, l'autre à la puissance μ, les coefficients de ces puissances étant des polynomes déterminés en u et v, c'est-à-dire *n'étant pas nuls quels que soient u et v*.

Si l'on exclut, par conséquent, les valeurs de u et v pour lesquelles ces coefficients s'annuleraient, l'on peut appliquer à F_1 et G_1 les résultats obtenus dans la théorie du résultant. D'une manière plus précise, nous savons former deux polynomes entiers $A(x, z, u, v)$ et $B(x, z, u, v)$ de degrés respectivement égaux à $\mu - 1$ et $\lambda - 1$ par rapport à x et tels qu'on ait l'identité en x et en z :

$$AF_1 + BG_1 = R(z, u, v),$$

R désignant un polynome entier en z, u et v qui n'est autre que le

résultant des polynomes F_1 et G_1. Faisons remarquer en passant que ce polynome est homogène par rapport aux trois lettres z, u et v et que son degré par rapport à z ne peut dépasser le produit $\lambda\mu$, ce qui est une conséquence immédiate des propriétés du résultant (*).

La relation $R(z, u, v) = 0$ à laquelle nous sommes ainsi parvenus d'une manière unique et déterminée et qui est une conséquence nécessaire des équations du système (1) a été appelée la *résolvante générale* de ce système ; nous allons en signaler ici les propriétés les plus importantes.

42. Nous observerons d'abord qu'il peut arriver que le polynome $R(z, u, v)$ qu'on appelle aussi quelquefois le *résolvant* du système (1), ne renferme pas z. Il se réduira par conséquent à un polynome entier en u et v, $P(u, v)$, et il nous est facile d'établir que ce polynome ne peut être identiquement nul. Si l'on avait en effet l'identité en x, z, u, v :

$$AF_1 + BG_1 = 0,$$

on pourrait en conclure que F_1 et G_1 ont, quels que soient u et v, un diviseur commun renfermant x, ce qui est contraire à l'hypothèse faite au début sur $F(x, y)$, et $G(x, y)$.

Il existe donc des valeurs de u et de v pour lesquelles le polynome $P(u, v)$ est différent de zéro, et par conséquent les relations

$$(1) \qquad F(x, y) = 0, \qquad G(x, y) = 0$$

nous conduisent à une contradiction. On en conclut que ces relations sont *incompatibles*, c'est-à-dire qu'il ne peut exister de symboles x et y possédant les modes de composition que nous avons imposés à x et y, qui vérifient les deux relations

$$F(x, y) = 0, \qquad G(x, y) = 0.$$

Un exemple simple de cette circonstance, auquel tous les autres peuvent d'ailleurs se ramener, s'obtient lorsqu'on suppose identi-

(*) Si l'on considère en effet les polynomes en x, $F_1(x, z, u, v)$ et $G_1(x, z, u, v)$, on voit qu'après division du premier par v^λ et du second par v^μ, les coefficients de x^i sont de degré égal à $-i$ par rapport à l'ensemble des lettres z, u et v ; le résolvant des deux polynomes ainsi obtenus est donc de degré $-\lambda\mu$ par rapport à l'ensemble de ces lettres. Il suffit d'observer que multiplier l'un des deux polynomes par v^λ et l'autre par v^μ équivaut à multiplier leur résolvant par $v^{2\lambda\mu}$ pour retrouver un résolvant *entier* en u, v et z et de dimension $\lambda\mu$.

quement

$$G(x, y) = F(x, y) + a,$$

a étant un nombre entier autre que zéro.

Ce cas étant écarté, nous allons étudier les propriétés du résolvant en supposant en premier lieu que tous les diviseurs irréductibles de ce résolvant sont différents ; en d'autres termes, *le polynome en* z $R(z, u, v)$ *est sans diviseurs multiples lorsque* u *et* v *demeurent indéterminés.*

La relation $R(z, u, v) = 0$, où l'on regarde z comme ayant été mis pour abréger à la place de $ux + vy$, est une identité en u et en v ; si nous y remplaçons u par $u + u'$ et v par $v + v'$, nous obtiendrons par conséquent une identité en u, v et aussi en u' et v', identité qui sera une conséquence nécessaire de la première. Considérons plus particulièrement les deux identités en u et v qu'on obtient en égalant à zéro les coefficients de u' et v' dans le développement du polynome

$$R[(u + u')x + (v + v')y, \quad u + u', \quad v + v'] ;$$

ces deux identités s'écrivent

$$D_u R(ux + vy, u, v) = 0,$$
$$D_v R(ux + vy, u, v) = 0,$$

en désignant par les premiers membres les polynomes dérivés du polynome $R(ux + vy, u, v)$ regardé successivement comme un polynome en u et comme un polynome en v. On voit d'ailleurs aisément d'après la définition des polynomes dérivés, que l'on peut écrire ces deux identités sous la nouvelle forme :

$$xD_z R(z, u, v) + D_u R(z, u, v) = 0,$$
$$yD_z R(z, u, v) + D_v R(z, u, v) = 0,$$

où la combinaison $z = ux + vy$ a été mise en évidence. Le système des trois identités en u et v :

$$(A) \begin{cases} R(z, u, v) = 0, \\ xD_z R(z, u, v) + D_u R(z, u, v) = 0, \\ yD_z R(z, u, v) + D_v R(z, u, v) = 0 \end{cases}$$

mérite de fixer un instant notre attention.

Nous ferons d'abord remarquer que lorsqu'on y regarde u et v

comme des entiers *déterminés*, les trois relations ainsi obtenues ne sont point distinctes ; c'est ce qui résulte de la relation

$$zD_zR(z, u, v) + uD_uR(z, u, v) + vD_vR(z, u, v) = 0,$$

relation qui d'une part est une combinaison linéaire des deux dernières relations du système (A) et qui d'autre part, d'après l'homogénéité du résolvant, est visiblement identique à la première de ces relations.

Cela étant acquis, considérons l'identité en u et v

$$R(ux + vy, u, v) = 0 ;$$

nous savons que le résolvant est homogène en u, v et z, nous pouvons donc en conclure que le polynome $R(ux + vy, u, v)$ est homogène en u et v. Si nous avons par conséquent, en posant $v = 1$,

$$R(ux + y, u, 1) = M_0(x, y) + uM_1(x, y) + u^2M_2(x, y) + \cdots,$$

l'identité $R(ux + vy, u, v) = 0$ est équivalente au système des relations

$$M_0(x, y) = 0, \qquad M_1(x, y) = 0, \ldots$$

obtenues en égalant à zéro les coefficients des diverses puissances de u. Si nous remarquons d'autre part que $R(z, u, v)$ est une combinaison linéaire des deux polynomes $F_1(x, z, u, v)$, $G_1(x, z, u, v)$, et par suite aussi des deux polynomes $F(x, y)$ et $G(x, y)$ auxquels ils se réduisent, au facteur v^λ ou v^μ près, nous pourrons en conclure que les polynomes M_i sont des fonctions linéaires et homogènes à coefficients entiers des deux polynomes $F(x, y)$ et $G(x, y)$. Ainsi toutes les relations $M_i = 0$ sont séparément des conséquences nécessaires des deux relations données dont elles sont des combinaisons linéaires.

Envisageons maintenant les deux dernières identités du système (A) ; elles s'obtiennent en dérivant la première soit par rapport à u soit par rapport à v, lorsqu'on y a remplacé z par l'expression $ux + vy$. Si l'on y fait $v = 1$, les coefficients des diverses puissances de u dans leurs premiers membres sont par conséquent, à des facteurs entiers près, les polynomes M_i déjà considérés. Toutes les relations (A) sont donc, quels que soient les entiers u et v, des combinaisons linéaires des relations $M_i = 0$ et par suite aussi des combinaisons linéaires des deux relations données

$$F(x, y) = 0, \qquad G(x, y) = 0.$$

Remplaçons dans les relations (A), u et v par des entiers déterminés a et b choisis de telle sorte que le polynome en z, $R(z, a, b)$, n'ait point de diviseurs multiples. Il suffit pour cela de choisir a et b de façon que le discriminant de ce polynome, qui est un polynome entier en u et v à coefficients entiers, soit différent de zéro. Considérons alors le système

$$(\mathrm{A})\qquad \left\{\begin{array}{l} R(z, a, b) = 0, \\ xD_zR(z, a, b) + D_aR(z, a, b) = 0, \\ yD_zR(z, a, b) + D_bR(z, a, b) = 0, \end{array}\right.$$

où z représente la combinaison $ax + by$; nous allons montrer que ce système est équivalent au système donné. Il nous suffira évidemment pour cela d'établir que les relations données sont des conséquences nécessaires des relations (A), puisque la réciproque a déjà été établie.

D'après l'hypothèse, les polynomes $R(z, a, b)$ et $D_zR(z, a, b)$ sont premiers entre eux ; il existe donc deux polynomes entiers en z, à coefficients entiers, $A(z)$ et $B(z)$, tels que l'on ait identiquement

$$A(z).R(z, a, b) + B(z).D_zR(z, a, b) = p,$$

p étant un nombre entier différent de zéro, qui est le discriminant de $R(z, a, b)$. On peut donc remplacer le système (A) par le suivant :

$$(\mathrm{A}')\qquad \left\{\begin{array}{l} R(z, a, b) = 0, \\ px + B(z).D_aR(z, a, b) = 0, \\ py + B(z).D_bR(z, a, b) = 0, \end{array}\right.$$

qui lui est manifestement équivalent.

Cela étant admis, lorsque la relation $R(z, a, b) = 0$ est satisfaite, les deux polynomes entiers en x : $F_1(x, z, a, b)$ et $G_1(x, z, a, b)$ ont nécessairement un diviseur commun renfermant x. Ce diviseur devant diviser toute combinaison linéaire des polynomes considérés sera par conséquent, à un facteur entier près, identique au polynome $px + B(z).D_aR(z, a, b)$; en d'autres termes, si nous prenons par exemple le reste de la division du polynome $p^{\lambda}F_1(x, z, a, b)$ par le binome en x : $px + B(z).D_aR(z, a, b)$, nous obtiendrons un polynome entier en z, à coefficients entiers, qui s'annulera sous la seule condition $R(z, a, b) = 0$. L'hypothèse faite au début sur

$R(z, a, b)$ nous permet d'en conclure que ce polynome $\Phi(z, a, b)$ est divisible par $R(z, a, b)$.

Considérons en effet un diviseur irréductible de $R(z, a, b)$ et désignons-le par $P(z, a, b)$; la relation $P(z, a, b) = 0$ entraîne nécessairement $\Phi(z, a, b) = 0$. Il est dès lors impossible que $\Phi(z, a, b)$ et $P(z, a, b)$ soient premiers entre eux, car l'identité en z que l'on pourrait alors écrire

$$A'(z).P(z, a, b) + B'(z).\Phi(z, a, b) = p',$$

où p' est un entier différent de zéro, est contradictoire avec la conclusion précédente. On peut donc affirmer que $\Phi(z, a, b)$ est divisible par $P(z, a, b)$ et que par conséquent le polynome $\Phi(z, a, b)$ qui admet tous les diviseurs irréductibles distincts de $R(z, a, b)$ est divisible par ce dernier polynome supposé sans diviseurs multiples.

Il existe donc une identité en z, de la forme

$$p^{\lambda}F_1(x, z, a, b) = N_1(z).R(z, a, b) + N_2(z, x)(px + B(z)).D_aR(z, a, b),$$

et cette identité exprime qu'à un facteur entier près, $F(x, y)$ est une combinaison linéaire des premiers membres des relations (A′) ou encore des relations (A). La démonstration s'applique évidemment aussi à $G(x, y)$.

Ainsi, *non seulement tout système de deux relations* $F(x, y) = 0$, $G(x, y) = 0$ *dont le résolvant est sans diviseurs multiples est équivalent au système formé des deux relations*

$$R(z, a, b) = 0,$$

$$xD_zR(z, a, b) + D_aR(z, a, b) = 0,$$

dans lesquelles z représente l'expression $ax + by$, *sous la seule condition que le polynome* $R(z, a, b)$ *soit sans diviseurs multiples, mais encore toute relation qui fait partie de l'un des deux systèmes est une combinaison linéaire des relations de l'autre système.*

Il est bien évident qu'il résulte également de là que les équations données sont des combinaisons linéaires des relations

$$M_i(x, y) = 0$$

considérées plus haut, de telle sorte que le système donné est aussi équivalent au système formé par ces relations.

43. Les propositions précédentes nous ont montré la liaison intime qui existe entre un système de deux relations entre x et y

et son résolvant dans le cas où ce dernier n'a que des diviseurs distincts. Il est aisé de voir comment on doit les modifier lorsque le résolvant $R(z, u, v)$ possède des diviseurs multiples.

Nous ferons observer qu'au point de vue où nous nous plaçons de la recherche des relations entières en x et y qui sont des conséquences nécessaires des relations données :

$$F(x, y) = 0, \qquad G(x, y) = 0,$$

nous pouvons substituer à la relation $R(z, u, v) = 0$ celle que l'on obtient en égalant à zéro le résolvant *débarrassé de ses facteurs multiples*, c'est-à-dire divisé par le plus grand commun diviseur à $R(z, u, v)$ et à $D_z R(z, u, v)$.

Si l'on désigne par $S(z, u, v)$ le quotient de cette division, le système

$$(B) \qquad \begin{cases} S(z, u, v) = 0, \\ xD_z S(z, u, v) + D_u S(z, u, v) = 0, \\ yD_z S(z, u, v) + D_v S(z, u, v) = 0, \end{cases}$$

où l'on regarde toujours z comme représentant $ux + vy$, pourra remplacer le système (A).

En particulier si le polynome $S(z, a, b)$ n'a point de diviseurs multiples, les deux relations

$$S(z, a, b) = 0,$$

$$xD_z S(z, a, b) + D_a S(z, a, b) = 0$$

nous donneront par de simples combinaisons linéaires toutes les conséquences nécessaires des relations données et en particulier ces relations elles-mêmes. Le système donné et le système (B) sont donc encore équivalents, c'est-à-dire conduisent aux mêmes conséquences relativement à x et à z, mais les relations du système (B), en particulier la première, ne sont plus simplement des combinaisons linéaires des relations données.

A un autre point de vue, si l'on s'astreint à ne considérer que les conséquences nécessaires des relations données qui en dérivent par des combinaisons linéaires, on parviendra naturellement à la relation $R(z, u, v) = 0$ et par suite aussi à toutes celles qui s'en déduisent en écrivant l'identité en u' et v'

$$R[(u + u')x + (v + v')y, \quad u + u', \quad v + v'] = 0$$

et qui en sont d'ailleurs des conséquences nécessaires, mais il est

en général impossible d'obtenir ainsi la relation $S(z, u, v) = 0$ et toutes celles qui en dérivent. Nous n'insisterons pas sur ce sujet qui demanderait une étude beaucoup plus profonde dépassant le cadre de ces leçons.

44. Nous avons jusqu'à présent supposé égal à deux le nombre des relations données entre x et y : il est aisé de montrer comment les résultats obtenus se peuvent étendre au cas où le nombre des relations données est quelconque.

Soient

$$G_1(x, y) = 0, \qquad G_2(x, y) = 0, \qquad \dots \qquad G_p(x, y) = 0$$

les relations données, entières et à coefficients entiers, desquelles nous supposerons seulement que leurs premiers membres n'ont point de diviseur commun. Désignons par $\alpha_1, \alpha_2, \dots, \alpha_p$; $\beta_1, \beta_2, \dots, \beta_p$ des nombres entiers dont nous ne fixons pas la détermination ; il est clair que les deux relations

$$\text{(I)} \qquad \left\{ \begin{array}{l} \alpha_1 G_1 + \dots + \alpha_p G_p = 0, \\ \beta_1 G_1 + \dots + \beta_p G_p = 0 \end{array} \right.$$

sont, quels que soient ces nombres, des conséquences nécessaires des relations données et que si l'on y laisse les α et les β indéterminés, elles entraineront nécessairement toutes ces relations. En d'autres termes, le système formé par ces deux relations est, *lorsque les α et les β sont indéterminés*, équivalent au système donné. Si l'on observe que leurs premiers membres sont sans diviseur commun et même irréductibles dans cette hypothèse, on pourra les traiter comme on l'a fait pour les deux équations

$$F(x, y) = 0, \qquad G(x, y) = 0.$$

Soit par conséquent $H(z, u, v, \alpha_i, \beta_k)$ le résolvant du système (I); la relation $H(z, u, v, \alpha_i, \beta_k) = 0$, dans laquelle z représente l'expression $ux + vy$, est une identité par rapport à u, v, aux α et aux β ; elle est d'ailleurs une combinaison linéaire des relations données et par suite une conséquence nécessaire de ces relations. Développons son premier membre suivant les puissances des α et des β et égalons à zéro les coefficients de ces diverses puissances ; nous obtiendrons un système d'identités en u et v,

$$K_1(z, u, v) = 0, \qquad K_2(z, u, v) = 0, \dots$$

qui sont également des combinaisons linéaires des relations données. Les polynomes $K(z, u, v)$ peuvent avoir ou non, lorsque u et v demeurent indéterminés, un diviseur commun renfermant z. Supposons d'abord que le dernier cas se présente ; il existera des polynomes entiers en z, u, v, tels qu'on ait identiquement

$$A_1(z, u, v).K_1(z, u, v) + A_2(z, u, v).K_2(z, u, v) + \cdots = P(u, v),$$

P étant un polynome entier en u et v. Il suffit de choisir pour u et v des entiers a et b qui n'annulent point le second membre, pour conclure de là qu'il est impossible que les relations

$$K_1(ax + by, a, b) = 0, \qquad K_2(ax + by, a, b) = 0, \ldots$$

aient lieu simultanément. Les relations données entre x et y sont donc incompatibles avec les hypothèses faites sur les symboles x et y.

Considérons maintenant le cas où les polynomes $K(z, u, v)$ ont un diviseur commun $R(z, u, v)$; il sera possible de déterminer des polynomes entiers en z, u, v tels qu'on ait identiquement

$$A_1(z, u, v).K_1(z, u, v) + A_2(z, u, v).K_2(z, u, v) + \cdots = R(z, u, v),$$

de sorte que la relation $R(z, u, v) = 0$, dans laquelle z représente toujours $ux + vy$, est une combinaison linéaire des relations $K(z, u, v) = 0$ et par suite aussi une combinaison linéaire des relations données.

Nous dirons que le polynome $R(z, u, v)$, auquel nous sommes ainsi parvenus d'une manière bien déterminée, est le *résolvant* du système donné. Il est aisé de voir qu'il possède toutes les propriétés du résolvant d'un système formé de deux relations seulement

En particulier si pour $u = a$, $v = b$ il est sans diviseurs multiples, ce qui ne peut arriver que dans le cas où il a, lorsque u et v sont indéterminés, ses diviseurs distincts, le système des relations

$$\text{(A)} \qquad \begin{cases} R(z, a, b) = 0, \\ xD_zR(z, a, b) + D_aR(z, a, b) = 0, \\ yD_zR(z, a, b) + D_bR(z, a, b) = 0 \end{cases}$$

est lié au système donné de telle sorte que toute relation d'un des systèmes est une combinaison linéaire des relations de l'autre système. Dans tous les cas, si $S(z, u, v)$ désigne le résolvant débar-

rassé de ses facteurs multiples, le système

$$\text{(B)} \qquad \begin{cases} S(z, u, v) = 0, \\ x D_z S(z, u, v) + D_u S(z, u, v) = 0, \\ y D_z S(z, u, v) + D_v S(z, u, v) = 0 \end{cases}$$

est équivalent au système donné, c'est-à-dire conduit aux mêmes conséquences relativement à x et à y.

Nous ne nous attarderons pas à refaire les démonstrations, qui se déduisent facilement de celles données dans le cas de deux équations, et nous passerons à une notion très importante pour la suite, celle des *systèmes irréductibles*.

45. Considérons un système de relations

$$G_1(x, y) = 0, \ldots, \qquad G_p(x, y) = 0$$

dont le résolvant $R(z, u, v)$ est supposé sans diviseurs multiples lorsque u et v demeurent indéterminés. Nous avons vu que la relation $R(ux + vy, u, v) = 0$ est, quels que soient u et v, une conséquence *nécessaire* des relations données, et que si l'on pose

$$R(ux + y, u, 1) = M_0(x, y) + uM_1(x, y) + u^2M_2(x, y) + \cdots$$

le système des relations

$$M_0(x, y) = 0, \qquad M_1(x, y) = 0, \ldots$$

est lié au système donné de telle sorte que toute relation de l'un des systèmes est une combinaison linéaire des relations de l'autre. Enfin, il est évident que le polynome $R(z, u, v)$ est également le résolvant de ce dernier système.

Une circonstance bien remarquable, que nous avons déjà admise implicitement en supposant que le résolvant possède quelquefois des diviseurs multiples, se présente ici. Il peut arriver, bien que les relations données entre x et y soient toutes irréductibles, qu'il n'en soit pas de même du résolvant. Considérons dans cette hypothèse l'un des diviseurs irréductibles $P(z, u, v)$ de $R(z, u, v)$, et soit

$$R(z, u, v) = P(z, u, v) . Q(z, u, v).$$

L'identité en u et v $R(z, u, v) = 0$ se décompose en deux identités : $P(z, u, v) = 0$, $Q(z, u, v) = 0$, qui sont nécessairement vérifiées *l'une ou l'autre*, lorsque les relations données sont satis-

faites. Ces deux identités sont d'ailleurs incompatibles, puisque les polynomes $P(z, u, v)$ et $Q(z, u, v)$ sont sans diviseur commun lorsque u et v demeurent indéterminés. Les conséquences nécessaires des relations $M(x, y) = 0$ ou des relations données se partagent donc en conséquences nécessaires de l'identité

$$P(ux + vy, u, v) = 0$$

et en conséquences nécessaires de l'identité

$$Q(ux + vy, u, v) = 0;$$

on dit que le système donné *se décompose*. Si l'on a alors

$$P(ux + y, u, 1) = K_0(x, y) + uK_1(x, y) + \cdots,$$

$$Q(ux + y, u, 1) = L_0(x, y) + uL_1(x, y) + \cdots,$$

on en déduit identiquement en x et y :

$$M_0 = K_0L_0,$$

$$M_1 = K_0L_1 + K_1L_0,$$

$$M_2 = K_0L_2 + K_1L_1 + K_2L_0,$$

et ces identités nous montrent pourquoi et comment la décomposition se produit.

Il semble inutile d'ajouter que $P(ux + vy, u, v)$ est précisément le résolvant du système

$$K_0(x, y) = 0, \qquad K_1(x, y) = 0, \ldots,$$

qui correspond au diviseur irréductible $P(z, u, v)$ et que l'on peut séparer du système donné. On voit d'ailleurs manifestement qu'en raisonnant sur le polynome $Q(z, u, v)$ comme on a raisonné sur $R(z, u, v)$ et ainsi de suite, il est possible de substituer à la considération de tout système *dont le résolvant est sans facteurs multiples*, celle d'un certain nombre de systèmes dont le résolvant est irréductible. Nous donnerons à ces derniers le nom de *systèmes irréductibles* et nous allons en signaler ici une propriété caractéristique, extrêmement importante.

Lorsqu'on envisage un système quelconque de relations entières entre x et y, dont le résolvant est dépourvu de diviseurs multiples sans être cependant irréductible, on voit immédiatement qu'il existe des relations entières en x et y qui, sans être incompatibles avec les relations données, n'en sont point pourtant

des conséquences *nécessaires*. Il est clair en effet que si l'on ajoute aux relations données la relation

$$P(ax + by, a, b) = 0,$$

en désignant par $P(z, u, v)$ l'un des facteurs irréductibles du résolvant, on forme un nouveau système dont le résolvant renfermera certainement le facteur $P(z, u, v)$ et qui se réduira à ce facteur lorsque les entiers a et b sont choisis de telle sorte que le polynome en z, $P(z, a, b)$ n'ait point de diviseurs multiples.

Mais supposons maintenant que le système donné soit irréductible, c'est-à-dire que son résolvant soit précisément $P(z, u, v)$ et ajoutons aux relations données une relation entière quelconque,

$$M(x, y) = 0.$$

Considérons le système ainsi obtenu et formons son résolvant ; il peut arriver que ce résolvant ne renferme pas z et nous pourrons alors affirmer que la relation $M(x, y) = 0$ est incompatible avec les relations données. Supposons que le cas contraire se présente et soit $P_1(z, u, v)$ le résolvant du nouveau système ; on voit que la relation $P(z, u, v) = 0$ sera une conséquence nécessaire de la relation $P_1(z, u, v) = 0$, d'où il résulte que P_1 et P sont identiques. On conclut de là que la relation $M(x, y) = 0$ est elle-même une conséquence nécessaire des relations données et même une combinaison linéaire de ces relations. Nous pouvons donc énoncer la proposition suivante : *Toute relation entière en x et y compatible avec les relations qui définissent un système irréductible est une conséquence nécessaire et même une combinaison linéaire de ces dernières.*

Cette propriété, avons-nous dit, *caractérise* les systèmes irréductibles ; nous avons en effet montré qu'étant donné un système quelconque non irréductible, on peut former des relations entières en x et y à coefficients entiers, qui sans être incompatibles avec les relations du système n'en sont pas cependant des conséquences nécessaires. Il est donc permis de définir les systèmes irréductibles en disant que pour ces systèmes *toute relation entière en x et y, à coefficients entiers, compatible avec les équations du système, en est nécessairement une combinaison linéaire ;* on reconnaît d'ailleurs là la généralisation d'une propriété caractéristique bien connue des polynomes irréductibles.

Signalons encore une conséquence immédiate des remarques pré-

cédentes : Soit $P(z, u, v)$ le résolvant irréductible d'un système d'équations entre x et y ; remplaçons dans ce polynome u et v par des entiers déterminés a et b. Il peut arriver que le polynome $P(z, a, b)$ possède ou non des diviseurs multiples, mais ce qui est remarquable c'est que :

1° *Lorsque* $P(z, a, b)$ *n'a pas de diviseurs multiples, il est nécessairement irréductible ;*

2° *Lorsque* $P(z, a, b)$ *a des diviseurs multiples, il est la puissance exacte d'un polynome irréductible.*

On observe en effet que dans le cas contraire, il serait possible d'écrire des relations de la forme $Q(ax + by, a, b) = 0$ compatibles avec les équations du système sans en être des conséquences nécessaires.

Enfin on peut affirmer que lorsque $P(z, a, b)$ est la puissance parfaite d'un polynome irréductible, ce dernier est une combinaison linéaire des premiers membres des équations du système.

IV. — Systèmes d'équations : Cas général.

46. Les résultats acquis dans l'étude des systèmes d'équations entre deux symboles x et y peuvent aisément s'étendre à des systèmes formés d'un nombre quelconque d'équations entre des symboles $x_1, x_2, \ldots, x_n$. Nous allons le montrer rapidement, sans insister sur des démonstrations qui sont identiques à celles que nous avons données dans le cas où l'on considère seulement deux symboles.

Soient

$$F_1(x_1, x_2, \ldots, x_n) = 0,$$
$$F_2(x_1, x_2, \ldots, x_n) = 0,$$
$$\cdots\cdots\cdots$$
$$F_p(x_1, x_2, \ldots, x_n) = 0$$

les relations qu'on suppose satisfaites par les symboles $x_1, x_2, \ldots, x_n$ et dans lesquelles F_i désigne un polynome entier à coefficients entiers de degré λ_i par rapport à l'ensemble des symboles qui y figurent. Nous observerons immédiatement qu'on pourrait, sans restreindre la généralité, se borner à étudier les systèmes de cette

forme dans lesquels les polynomes F sont irréductibles; la raison de ce fait est évidemment la même que dans le cas de deux symboles x et y; néanmoins comme l'on peut sans introduire de complications arriver à un certain nombre de résultats sans faire cette hypothèse, nous ne la ferons pas tout d'abord.

Nous allons poser, comme dans le cas de deux symboles,

$$z = u_1x_1 + u_2x_2 + \ldots + u_nx_n,$$

en désignant par $u_1, u_2, \ldots, u_n$ des entiers indéterminés qu'on s'astreint à ne jamais choisir nuls simultanément, et rechercher les propriétés du symbole z ainsi défini. Désignons à cet effet par

$$\Phi_i(x_1, x_2, \ldots, x_{n-1}, z)$$

le polynome entier en $x_1, x_2, \ldots, x_{n-1}, z$ et $u_1, u_2, \ldots, u_n$ que l'on déduit du polynome $F_i(x_1, x_2, \ldots, x_n)$ en multipliant ce dernier par $u_n^{\lambda_i}$ et en y remplaçant ensuite u_nx_n par l'expression

$$z - u_1x_1 - \ldots - u_{n-1}x_{n-1};$$

les relations

$$\Phi_i(x_1, x_2, \ldots, x_{n-1}, z) = 0$$
$$(i = 1, 2, \ldots, p)$$

sont, lorsqu'on suppose u_n différent de zéro, des conséquences nécessaires des relations données, et la réciproque est également vraie. Nous ferons remarquer que ces relations ne renferment pas nécessairement toutes le symbole z — il est clair en effet que si le polynome F_i ne contient pas x_n, le polynome Φ_i ne renfermera pas z — mais il importe d'observer que lorsque Φ_i renferme effectivement z, Φ_i est un polynome en $x_1, x_2, \ldots, x_{n-1}$ dont le degré par rapport à chacune de ces lettres est égal à λ_i, dimension maximum du polynome Φ_i considéré comme polynome en $x_1, x_2, \ldots, x_{n-1}$ et z. On voit également que Φ_i est *homogène* et de degré λ_i par rapport aux lettres $u_1, u_2, \ldots, u_n$ et z, sans être nécessairement de degré λ_i par rapport à z.

Considérons les polynomes en z, $\Phi_i(x_1, x_2, \ldots, x_{n-1}, z)$ et formons leur plus grand commun diviseur; ce plus grand commun diviseur n'existera évidemment que lorsque tous les polynomes Φ_i renferment effectivement z; mais nous pouvons affirmer que s'il existe, il renfermera également les symboles $x_1, x_2, \ldots, x_{n-1}$. On s'en convaincra immédiatement si l'on observe qu'il dérive du plus

grand commun diviseur des polynomes en x_n, désignés par F_i, en y remplaçant après multiplication par une puissance convenable de u_n, $u_n x_n$ par la différence

$$u_1 x_1 + \ldots + u_{n-1} x_{n-1} - z.$$

Désignons donc ce plus grand commun diviseur par

$$R_1(z, x_1, \ldots, x_{n-1});$$

si nous appelons $G_i(x_1, x_2, \ldots, x_{i-1}, z)$ le quotient de Φ_n par R_1, les relations

$$\Phi_i = 0 \qquad (i = 1, 2, \ldots, p)$$

pourront s'écrire

$$R_1 G_i = 0 \qquad (i = 1, 2, \ldots, p).$$

Leurs conséquences nécessaires se partagent donc en conséquences nécessaires de la relation $R_1 = 0$ et en conséquences nécessaires des p relations $G_i = 0$ $(i = 1, 2, \ldots, p)$: il est d'ailleurs évident que lorsque les relations de l'un ou de l'autre de ces derniers systèmes sont vérifiées, il en est de même des relations

$$\Phi_i = 0 \qquad (i = 1, 2, \ldots, p).$$

Le système donné *se décompose* donc en deux systèmes dont l'un est constitué par l'unique relation entre n symboles

$$R_1(z, x_1, x_2, \ldots, x_{n-1}) = 0,$$

et l'autre par les p relations

$$G_i(x_1, x_2, \ldots, x_{n-1}, z) = 0$$

$$(i = 1, 2, \ldots, p),$$

dans lesquelles les polynomes en z qui forment les premiers membres sont sans diviseur commun.

Considérons ce dernier système ; nous observerons que si l'un des polynomes G_i renferme l'un des symboles $x_1, x_2, \ldots, x_{n-1}$, il les renfermera nécessairement tous et sera en outre par rapport à chacun d'eux de degré égal à sa dimension maximum ; c'est là une conséquence immédiate de la propriété correspondante des polynomes Φ_i.

Examinons le cas où aucun des polynomes G_i ne renferme de symboles $x_1, x_2, \ldots, x_{n-1}$; nous pouvons affirmer que ces polynomes qui ne renferment plus que z et qui sont, lorsque les u sont indéterminés, sans diviseur commun, ne peuvent s'annuler simul-

tanément quels que soient les u. Les relations

$$G_i(z) = 0 \qquad (i = 1, 2, \ldots, p),$$

considérées comme relations en $x_1, x_2, \ldots, x_n$, devant avoir lieu quels que soient les u, sont par conséquent incompatibles.

Ce cas étant écarté, il peut arriver qu'aucun des polynomes G_i qui renferment effectivement $x_1, x_2, \ldots, x_{n-1}$, ne renferme z ; le système formé des relations $G_i = 0$, $(i = 1, 2, \ldots, p)$ est alors un système de p équations entre les $(n-1)$ symboles

$$x_1, x_2, \ldots, x_{n-1},$$

et ces équations doivent avoir lieu quels que soient les entiers indéterminés $u_1, u_2, \ldots, u_n$. Il suffit par conséquent de développer les G_i suivant les puissances des u et d'égaler à zéro les coefficients de ces diverses puissances, pour obtenir un système d'équations à coefficients entiers entre les $(n-1)$ symboles $x_1, x_2, \ldots, x_{n-1}$. On appliquera alors à ce système la méthode que l'on vient d'appliquer au système donné qui renfermait effectivement n symboles. Il est aisé de voir que ce cas ne se présente que lorsque les polynomes F_i ne renferment x_n que par un facteur qui est le même pour tous ces polynomes.

Dans tous les autres cas, nous pouvons affirmer que le système des relations

$$G_i(x_1, x_2, \ldots, x_{n-1}, z) = 0$$
$$(i = 1, 2, \ldots, p),$$

— qui se réduit au sytème

$$\Phi_i(x_1, x_2, \ldots, x_{n-1}, z) = 0$$
$$(i = 1, 2, \ldots, p)$$

lorsque les polynomes en z, représentés par les Φ_i, n'ont pas de diviseur commun — renferme au moins une relation dont le premier membre est un polynome en $x_1, x_2, \ldots, x_{n-1}$ et z, dont le degré par rapport à chacune des lettres $x_1, x_2, \ldots, x_{n-1}$ est égal à sa dimension maximum. Considérons alors les deux relations

$$\alpha_1 G_1 + \cdots + \alpha_p G_p = 0,$$

$$\beta_1 G_1 + \cdots + \beta_p G_p = 0,$$

dans lesquelles les α et les β représentent des entiers qu'on laisse indéterminés, ces deux relations sont toujours des conséquences

nécessaires des relations

$$G_i = 0 \qquad (i = 1, 2, \dots, p),$$

et il est clair que la réciproque est vraie, de sorte qu'on peut se borner à rechercher les conséquences nécessaires de ces deux relations dans lesquelles on suppose expressément que les α et les β demeurent indéterminés. Leurs premiers membres sont des polynomes entiers en $x_1, x_2, \dots, x_{n-1}$ et z, et nous savons qu'ils sont par rapport à x_{n-1} en particulier de degré égal à leur dimension maximum ; nous pouvons donc leur appliquer les résultats obtenus relativement au résultant de deux polynomes de degrés donnés. En d'autres termes, si nous désignons par

$$T(z, x_1, x_2, \dots, x_{n-2}, \alpha, \beta)$$

le résultant de ces polynomes considérés comme polynomes en x_{n-1}, la relation

$$T(z, x_1, x_2, \dots, x_{n-2}, \alpha, \beta) = 0$$

sera une conséquence nécessaire des relations

$$G_i = 0 \qquad (i = 1, 2, \dots, p).$$

Mais nous pouvons aller plus loin ; si l'on considère en effet le système formé des relations

$$G'_i = 0 \qquad (i = 1, 2, \dots, p),$$

qu'on déduit des relations $G_i = 0$ $(i = 1, 2, \dots, p)$ en y remplaçant z par son expression à l'aide des x, il est évident que le polynome

$$T(z, x_1, x_2, \dots, x_{n-2}, \alpha, \beta)$$

nous donne, lorsqu'on y remplace z par $z' + u_1x_1 + \dots + u_{n-2}x_{n-2}$, le résolvant des deux polynomes en x_{n-1} et x_n :

$$\alpha_1 G'_1 + \dots + \alpha_p G'_p,$$

$$\beta_1 G'_1 + \dots + \beta_p G'_p.$$

Nous pouvons donc dire que *si le polynome* T, qui renferme nécessairement $x_1, x_2, \dots, x_{n-2}$, *est sans diviseurs multiples lorsque* $x_1, x_2, \dots, x_{n-2}$ *ainsi que* u_n *et* u_{n-1} *demeurent indéterminés*, la relation

$$T(z, x_1, \dots, x_{n-2}, \alpha, \beta) = 0,$$

supposée vérifiée quels que soient u_n, u_{n-1} et les indéterminées α et β, conduit à toutes les conséquences nécessaires des relations

$$G_i = 0 \qquad (i = 1, 2, \ldots, p).$$

Si l'on développe par conséquent le polynome T suivant les puissances des α et des β, on obtiendra, en égalant à zéro les coefficients de ces diverses puissances, un système d'équations entre $(n-1)$ symboles seulement, $x_1, \ldots, x_{n-2}$ et z, qui sera équivalent au système

$$G_i = 0 \qquad (i = 1, 2, \ldots, p),$$

à la condition d'être vérifié quels que soient u_n et u_{n-1}. On peut d'ailleurs remarquer que les relations de chacun des systèmes sont simplement des combinaisons linéaires de celles de l'autre.

Supposons maintenant que le polynome T possède des diviseurs multiples lorsque $x_1, \ldots, x_{n-2}$, u_n et u_{n-1} demeurent indéterminés ; nous savons qu'il suffit de substituer à T le produit de ses facteurs irréductibles distincts pour obtenir un polynome T_1 auquel les conclusions précédentes s'appliquent. Il importe seulement d'observer que les équations du nouveau système entre les $(n-1)$ symboles $x_1, x_2, \ldots, x_{n-2}, z$, que l'on en déduit, ne sont plus de simples combinaisons linéaires des relations

$$G_i = 0 \qquad (i = 1, 2, \ldots, p).$$

Au point de vue où nous nous plaçons, il est indifférent d'avoir égard à l'ordre de multiplicité des diviseurs ; nous n'insisterons donc pas sur les circonstances qui peuvent se présenter dans le cas où il existe des diviseurs multiples.

Les remarques qui précèdent nous permettent, *dans tous les cas*, de remplacer les relations

$$G_i = 0 \qquad (i = 1, 2, \ldots, p)$$

par des relations

$$H_i = 0 \qquad (i = 1, 2, \ldots, q)$$

entre les $(n-1)$ symboles $x_1, x_2, \ldots, x_{n-2}$ et z ou bien entre les $(n-1)$ symboles $x_1, x_2, \ldots, x_{n-1}$. Nous pouvons même y supposer dans le cas où elles renferment z, les indéterminées $u_1, u_2, \ldots, u_{n-2}$ remplacées par des entiers quelconques, en particulier les faire toutes égales à zéro, sans que nos conclusions cessent d'être valables; cela résulte de ce que lorsqu'on pose

$$z = z_1 + u_1 x_1 + \cdots + u_{n-2} x_{n-2},$$

les indéterminées $u_1, u_2, \ldots, u_{n-2}$ disparaissent de ces relations où elles ne figuraient qu'en apparence.

Rien ne nous empêche maintenant de raisonner sur le système

$$H_i(x_1, \dots, x_{n-2}, z_1) = 0$$
$$(i = 1, 2, \dots, q)$$

comme on a raisonné sur le système d'où l'on est parti :

$$F_i(x_1, \dots, x_n) = 0$$
$$(i = 1, 2, \dots, p),$$

et ainsi de suite jusqu'à l'épuisement des $(n-2)$ symboles $x_1, x_2, \dots, x_{n-2}$.

On peut enfin observer que si z_1 désigne la combinaison $u_n x_n + u_{n-1} x_{n-1}$, dans laquelle u_n et u_{n-1} sont indéterminés, il est inutile d'introduire l'indéterminée v_{n-1} lorsqu'on forme la combinaison

$$z = v_1 x_1 + \dots + v_{n-2} x_{n-2} + v_{n-1} z_1 ;$$

on pourra donc conserver les mêmes notations pour les indéterminées et poser simplement

$$z = u_1 x_1 + \dots + u_{n-2} x_{n-2} + z_1,$$

c'est-à-dire partir de la considération des relations

$$H_i(x_1, x_2, \dots, x_{n-2}, z) = 0$$
$$(i = 1, 2, \dots, q)$$

telles qu'on les a obtenues directement.

Il est clair qu'en continuant ainsi on parviendra certainement à un système de relations renfermant seulement z et incompatibles lorsque les u demeurent indéterminés, système analogue à celui qui s'est présenté dès le début. On obtient par conséquent une suite de polynomes $R_i(x_1, \dots, x_{n-i}, z)$, suite qui peut être complète ou non, telle que lorsque les relations données

$$F_i(x_1, x_2, \dots, x_n) = 0$$
$$(i = 1, 2, \dots, p)$$

sont satisfaites, il en est de même de l'une au moins des relations

$$R_i(x_1, x_2, \dots, x_{n-i}, z) = 0,$$

quelles que soient les indéterminées $u_1, u_2, \dots, u_n$, la réciproque étant vraie.

On dit que l'équation

$$\prod R_i(x_1, \dots, x_{n-i}, z) = 0$$

est la *résolvante générale* du système d'équations donné, et une étude plus complète, que nous ne pouvons aborder dans ces leçons, montrerait comment sa considération conduit aux propriétés les plus importantes de ce système.

47. Nous voulons nous borner ici à l'étude des systèmes pour lesquels cette résolvante se réduit à un polynome en z : $R_n(z, u_1, u_2, \ldots, u_n)$, qui, lorsque les u sont indéterminés, est dépourvu de diviseurs multiples.

Nous établirons plus loin que les relations entre $x_1, x_2, \ldots, x_n$ qui constituent un pareil système suffisent pour fixer d'un nombre limité de manières distinctes le calcul des symboles $x_1, x_2, \ldots, x_n$, dont aucun ne peut par conséquent être choisi d'une manière arbitraire dans un ensemble de symboles connus; on reconnait là les systèmes *à solutions déterminées* dont il a été question au début de ce chapitre. Cela étant admis, on voit immédiatement que tout système dont la résolvante peut s'écrire

$$R_i(x_1, x_2, \ldots, x_{n-i}, z) = 0$$

devient un système à solutions déterminées lorsqu'on fixe d'une manière arbitraire $x_1, x_2, \ldots, x_{n-i}$ dans l'ensemble des nombres entiers; il suffit donc de considérer les systèmes dont la résolvante est de la forme

$$R_n(z, u_1, u_2, \ldots, u_n) = 0$$

pour obtenir tous les systèmes à solutions déterminées.

On peut répéter sur le polynome $R_n(z, u_1, u_2, \ldots, u_n)$, dans le cas où il n'admet point de diviseurs multiples, tout ce qui a été dit sur le résolvant dans le cas de deux symboles seulement. Il est aisé de voir que ce polynome est homogène en $u_1, u_2, \ldots, u_n$ et z et d'un degré d'homogénéité égal au produit des dimensions maxima des premiers membres des relations données :

$$F_i = 0 \qquad (i = 1, 2, \ldots, p),$$

bien qu'il puisse être par rapport à z de degré inférieur à ce produit.

Le polynome $R_n(z, u)$ est une combinaison linéaire des polynomes F_i, et lorsque les a sont des entiers choisis de telle sorte que le polynome en z, $R_n(z, a)$, ait ses diviseurs distincts, les

relations du système donné sont également des combinaisons linéaires des relations

$$R_n(z, a) = 0,$$
$$x_i D_z R_n(z, a) + D_{a_i} R_n(z, a) = 0$$
$$(i = 1, 2, \dots, n),$$

dont d'ailleurs n seulement sont distinctes.

A un autre point de vue, l'on voit également que toute décomposition du résolvant $R_n(z, u)$ conduit à une décomposition du système donné, ou en d'autres termes permet une séparation des diverses relations entières en $x_1, x_2, \dots, x_n$ à coefficients entiers qui sont compatibles avec les relations données. On est ainsi conduit à la considération de systèmes d'équations dont le résolvant est irréductible, et il est clair que la propriété caractéristique de ces systèmes, donnée dans le cas de deux symboles x et y, subsiste dans le cas général, autrement dit : *Lorsqu'un système est irréductible, toute relation entière en* $x_1, x_2, \dots, x_n$ *à coefficients entiers qui n'est pas incompatible avec les relations du système en est une combinaison linéaire, et réciproquement, lorsque toute relation entière en* $x_1, x_2, \dots, x_n$ *à coefficients entiers compatible avec les équations d'un système à solutions déterminées, en est une combinaison linéaire, c'est-à-dire une conséquence nécessaire, ce système est irréductible.*

Enfin il résulte également de là que lorsque $R_n(z, u)$ est irréductible, $R_n(z, a)$ est irréductible ou puissance d'un polynome irréductible qu'on peut obtenir par de simples combinaisons linéaires des premiers membres des équations du système.

CHAPITRE IV

LE CALCUL DES ENTIERS ALGÉBRIQUES

I. — Formation d'un domaine algébrique.

1re MÉTHODE.

48. Les développements dans lesquels nous sommes entrés au sujet des systèmes d'équations vont nous permettre de répondre aisément aux diverses questions qui se sont présentées au moment où nous avons défini les nombres algébriques. Ils nous suffiront, en particulier, pour établir que la définition qui a été donnée de ces symboles ne peut conduire à aucune contradiction et qu'elle suffit pour déterminer leur calcul (*) d'une manière unique. On aura ainsi démontré l'existence logique des nombres algébriques.

Rappelons que nous nous bornons toujours à considérer les nombres algébriques *entiers* desquels les autres se déduisent en les divisant par des entiers ordinaires.

Nous commencerons par montrer comment l'on peut définir d'une manière unique et déterminée le calcul des nombres algébriques entiers, dans tout domaine que l'on sait former par des adjonctions successives d'un seul symbole à un domaine dans lequel le calcul est déjà connu. Il est superflu d'ajouter que le calcul auquel nous parviendrons ne présentant jamais de contradiction, nous établissons ainsi l'existence logique de ceux des entiers algébriques qui appartiennent au domaine considéré.

(*) Nous entendons toujours par *calcul* les règles qui permettent de décider si deux symboles sont ou non distincts et de donner leur somme et leur produit.

Nous supposons par conséquent que l'on part du domaine formé par les nombres entiers ordinaires, domaine dans lequel le calcul est connu, et désignant par $f(x)$ un polynome irréductible à coefficients entiers dont le premier coefficient est l'unité, nous adjoindrons à ce domaine un symbole ξ, assujetti *d'une part* à se composer avec les entiers et aussi avec lui-même suivant deux modes distincts qui possèdent les propriétés fondamentales de l'addition et de la multiplication des entiers, et *d'autre part* à vérifier la relation $f(\xi) = 0$.

On a déjà établi que ces hypothèses permettent de construire des tables d'addition et de multiplication pour les fonctions entières de ξ à coefficients entiers et que tous les symboles distincts qui figurent parmi ces fonctions s'obtiennent et s'obtiennent une seule fois quand on considère seulement celles d'entre elles dont le degré est inférieur au degré m du polynome $f(x)$.

On peut donc dire que le calcul dans le domaine $[\xi]$ est déterminé d'une manière unique, complètement connu, et ne renferme point de contradiction; d'où il résulte qu'il est effectivement possible, au point de vue logique, de définir un symbole ξ par les conditions précédentes. C'est de cette possibilité que nous allons, en dernière analyse, faire dépendre l'existence logique des nombres algébriques.

Mais revenons à notre objet, qui est de former un domaine algébrique par des adjonctions successives d'un seul symbole à un domaine où le calcul est connu.

Considérons un symbole η, duquel nous supposerons qu'il possède, avec lui-même et les éléments du domaine $[\xi]$, les modes de composition imposés à ξ et qu'il vérifie en outre la relation irréductible à coefficients entiers

$$g(\eta) = 0,$$

où $g(y)$ désigne un polynome irréductible à coefficients entiers dont le premier coefficient est l'unité et que l'on suppose distinct du polynome $f(y)$. Proposons-nous maintenant de définir le calcul des fonctions entières de ξ et de η, à coefficients entiers, c'est-à-dire le calcul dans le domaine algébrique $[\xi, \eta]$ qui résulte de l'adjonction du symbole η au domaine $[\xi]$.

Il faudra en premier lieu chercher tous les éléments distincts qui figurent parmi les fonctions entières de ξ et de η, à coefficients

entiers, ce qui revient évidemment à chercher tous ceux de ces éléments qui sont égaux à zéro. On est ainsi conduit à rechercher toutes les relations entières en x et y à coefficients entiers qui sont *compatibles* avec les relations

(I) $$f(x) = 0, \qquad g(y) = 0;$$

nous voulons dire par là toutes les relations $M(x, y) = 0$ qui sont telles que le résolvant du système

$$f(x) = 0, \qquad g(y) = 0,$$
$$M(x, y) = 0$$

renferme effectivement z (nous conservons les notations du chapitre précédent). Il a été en effet établi que dans le cas contraire les trois relations qui précèdent sont contradictoires avec les hypothèses faites sur x et sur y.

49. Nous savons que la considération du résolvant du système (I) donne le moyen de former naturellement toutes ces relations; nous formerons par conséquent ce résolvant, c'est-à-dire qu'en supposant

$$f(x) = x^m + a_1 x^{m-1} + \cdots + a_m,$$
$$g(y) = y^p + b_1 y^{p-1} + \cdots + b_p,$$

nous formerons le résultant des deux polynomes en ux :

$$(ux)^m + a_1 u(ux)^{m-1} + \cdots + a_m u^m$$

et

$$(z - ux)^p + b_1 v(z - ux)^{p-1} + \cdots + b_p v^p.$$

Ce résultant est un polynome homogène en z, u et v dont le degré est mp et qui renferme effectivement z^{mp}; il est bon d'observer immédiatement que *ce polynome est sans diviseurs multiples lorsque u et v demeurent indéterminés*, c'est ce qu'il est facile d'établir.

On sait que si l'on considère les deux polynomes

$$\varphi(x) = (x + x_1)(x + x_2)\ldots(x + x_m),$$
$$\psi(y) = (y + y_1)(y + y_2)\ldots(y + y_p),$$

le produit $\psi(x_1).\psi(x_2)\ldots\psi(x_m)$ est symétrique par rapport aux x et aussi par rapport aux y, d'où il résulte qu'on peut l'exprimer *et d'une seule manière* à l'aide des fonctions symétriques élémentaires $S_1, S_2, \ldots, S_m$ des x et des fonctions symétriques élémentaires $T_1, T_2, \ldots, T_p$ des y; nous rappellerons en outre que ce produit est

composé avec les S et les T de la même manière que le résultant des deux polynomes

$$f(x) = x^m + a_1 x^{m-1} + \cdots + a_m,$$

$$g(x) = x^p + b_1 x^{p-1} + \cdots + b_p$$

est composé avec les coefficients a et b de ces polynomes. Il résulte de là que l'on parvient au résolvant du système

$$f(x) = x^m + a_1 x^{m-1} + \cdots + a_m = 0,$$

$$g(y) = y^p + b_1 y^{p-1} + \cdots + b_p = 0,$$

en remplaçant dans le produit des mp facteurs

$$\prod (z + ux_i + vy_k),$$

où i et k désignent successivement l'un, les entiers $1, 2, \ldots, m$, l'autre, les entiers $1, 2, \ldots, p$, d'une part les S par les a et d'autre part les T par les b.

Considérons ensuite le discriminant du résolvant qu'on vient de former ; une remarque analogue montre qu'on peut obtenir ce discriminant en remplaçant respectivement dans le produit de $mp(mp-1)$ facteurs

$$\prod [u(x_i - x_{i'}) + v(y_k - y_{k'})]$$

les fonctions symétriques élémentaires

$$S_1, S_2, \ldots, S_m \quad \text{et} \quad T_1, T_2, \ldots, T_p$$

par $a_1, a_2, \ldots, a_m$ et $b_1, b_2, \ldots, b_p$. Il est dès lors facile de donner l'expression d'un terme quelconque de ce discriminant ; nous observerons que le discriminant est homogène en u et v et de degré $mp(mp-1)$ et nous choisirons celui de ses termes qui renferme u à la plus haute puissance. On reconnaît immédiatement que ce terme est

$$u^{m(m-1)p^2} \cdot v^{p(p-1)m} \cdot \Delta_f^{p^2} \cdot \Delta_g^m,$$

en désignant par Δ_f le discriminant du polynome $f(x)$ et par Δ_g celui du polynome $g(y)$, et l'on peut conclure de là que *le discriminant du résolvant ne peut être nul, quels que soient u et v, que dans le cas où l'un des polynomes $f(x)$ et $g(y)$ a des diviseurs multiples*, ce qui démontre la propriété annoncée.

Nous n'avons donc à examiner que deux cas distincts suivant que le résolvant $R(z, u, v)$ est ou non irréductible.

Envisageons d'abord le premier d'entre eux, c'est-à-dire supposons le résolvant irréductible ; nous savons qu'alors toute relation entière en x et y, à coefficients entiers, $M(x, y) = 0$, qui est compatible avec les relations données, en est une conséquence *nécessaire* et même une combinaison linéaire. Désignons par a et b deux entiers tels que le polynome $R(z, a, b)$ n'ait point de facteurs multiples; nous savons également que le polynome $R(z, a, b)$ est irréductible et que les relations

$$\text{(II)} \qquad \begin{cases} R(z, a, b) = 0, \\ xD_zR(z, a, b) + D_aR(z, a, b) = 0, \\ yD_zR(z, a, b) + D_bR(z, a, b) = 0 \end{cases}$$

peuvent remplacer complètement les relations données. Enfin, si l'on observe que lorsque ξ et η vérifient les relations

$$f(\xi) = 0, \quad g(\eta) = 0,$$

le symbole $\zeta = a\xi + b\eta$ vérifie la relation

$$R(\zeta, a, b) = 0,$$

on voit que l'introduction dans le calcul des symboles ξ et η équivaut à l'introduction du symbole unique ζ, qui est également un nombre algébrique entier et qui est défini par la relation irréductible

$$R(\zeta, a, b) = 0.$$

Il est en effet inutile de rappeler que les relations (II) donnent dans ce cas l'expression de ξ et η comme fonctions entières de ζ *à coefficients entiers.*

Le domaine algébrique $[\xi, \eta]$ est donc identique au domaine $[\zeta]$ et dans ce dernier domaine le calcul est défini, d'une manière unique et déterminée, par les hypothèses faites sur ζ.

50. Examinons maintenant ce qui se passe lorsque le résolvant $R(z, u, v)$ n'est pas irréductible ; nous conviendrons de désigner par $P(z, u, v)$ l'un quelconque de ses diviseurs irréductibles. Les relations entières en x et y à coefficients entiers qui sont compatibles avec les deux relations

$$\text{(I)} \qquad f(x) = 0, \qquad g(y) = 0$$

sont, ou bien des conséquences nécessaires de ces relations, ou bien

des conséquences nécessaires des relations de l'un des systèmes

$$P(z, a, b) = 0,$$
$$xD_zP(z, a, b) + D_aP(z, a, b) = 0,$$
$$yD_zP(z, a, b) + D_bP(z, a, b) = 0,$$

dans lesquelles a et b sont des entiers choisis de telle sorte que le polynome $R(z, a, b)$ soit sans diviseurs multiples. Ces dernières relations forment d'ailleurs, lorsqu'on y regarde z comme représentant la combinaison $ax + by$, l'un quelconque des systèmes irréductibles en lesquels le système (I) peut être *décomposé*.

Il résulte de là que le calcul des fonctions entières de ξ et η à coefficients entiers n'est pas complètement déterminé par les hypothèses faites sur ces symboles, puisqu'on parvient à des conclusions différentes suivant qu'on admet que les relations de l'un ou de l'autre des systèmes irréductibles qu'on vient de former sont vérifiées par ces symboles. Mais on peut ajouter immédiatement que si l'on assujettit des symboles ξ et η à se composer entre eux et avec les entiers suivant les deux modes exigés et à vérifier les relations

$$P(\zeta, a, b) = 0,$$
$$\xi D_\zeta P(\zeta, a, b) + D_aP(\zeta, a, b) = 0,$$
$$\eta D_\zeta P(\zeta, a, b) + D_bP(\zeta, a, b) = 0,$$

où ζ désigne l'expression $a\xi + b\eta$, et qui comme on le sait se réduisent à deux relations distinctes seulement, ces conditions définissent d'une manière unique le calcul des symboles ξ et η.

Le calcul ainsi défini est identique à celui du seul symbole ζ assujetti à posséder avec les entiers et avec lui-même les mêmes modes de composition et à vérifier la relation irréductible $P(\zeta, a, b) = 0$. Enfin les symboles ξ et η déterminés par les relations précédentes vérifient les relations $f(\xi) = 0$, $g(\eta) = 0$, quel que soit le facteur irréductible du résolvant désigné par $P(z, u, v)$.

On reconnaît ainsi qu'*il existe différents couples d'entiers algébriques* (ξ, η) *qui satisfont aux deux relations*

$$f(\xi) = 0, \qquad g(\eta) = 0$$

et que *le calcul des fonctions entières à coefficients entiers de* ξ *et de* η *n'est pas le même pour tous ces couples.*

Nous sommes donc amenés à préciser, en partant d'un symbole ξ assujetti à vérifier la relation $f(\xi) = 0$, celui des symboles η qui

peuvent vérifier la relation $g(\eta) = 0$, que l'on veut adjoindre au domaine $[\xi]$. Nous venons de montrer qu'il suffit pour cela de donner le facteur irréductible $P(z, a, b)$ du résolvant qui doit s'annuler quand on y remplace z par la combinaison $a\xi + b\eta$. Cette opération étant faite, le calcul des entiers algébriques ξ et η est déterminé d'une manière unique; et nous avons établi qu'il est identique au calcul d'un seul symbole ζ — symbole qui est également un entier algébrique puisque $\zeta = a\xi + b\eta$ — assujetti à vérifier la relation irréductible

$$P(\zeta, a, b) = 0.$$

Il convient d'observer ici qu'on pouvait prévoir les résultats que nous venons d'obtenir. Il est évident en effet que pour être assuré de ne rencontrer dans le calcul des symboles ξ et η aucune ambiguïté, il est nécessaire et suffisant d'imposer à ces symboles des conditions telles que toutes les relations *compatibles* avec ces conditions en soient des conséquences *nécessaires*. Les relations par lesquelles nous définissons *le calcul de* ξ *et de* η *et par suite ces symboles eux-mêmes, en tant qu'ils nous sont accessibles*, doivent par conséquent former un système irréductible. Nous venons de voir comment il faut les choisir pour qu'il en soit ainsi.

En résumé, l'analyse précédente nous permet de remplacer dans tous les cas l'adjonction à l'ensemble des nombres entiers de deux entiers algébriques *bien définis* — et nous savons ce qu'il faut entendre par là — par celle d'un seul entier algébrique que l'on sait également définir d'une manière précise.

Nous pouvons donc conclure de là une manière de définir le calcul dans tout domaine $[\xi, \eta, \zeta, \ldots\ldots]$ formé par des entiers algébriques qui vérifient les relations irréductibles à coefficients entiers

$$f(\xi) = 0, \qquad g(\eta) = 0, \qquad h(\zeta) = 0, \qquad \ldots\ldots$$

à condition de préciser *si cela est nécessaire,* comme on a appris à le faire, la définition du symbole que l'on veut adjoindre à un domaine dans lequel le calcul est déterminé d'une manière unique. Il est inutile d'ajouter que le calcul ainsi défini ne renfermera aucune contradiction puisqu'il est identique au calcul dans un domaine algébrique $[\alpha]$, où l'entier algébrique α est défini par une seule relation irréductible à coefficients entiers,

$$R(\alpha) = 0,$$

que nous avons appris à former.

51. Revenons aux relations

$$(\text{I}) \qquad \begin{cases} f(\xi) = 0, \; g(\eta) = 0, \\ \text{P}(\zeta, a, b) = 0, \end{cases}$$

où ζ représente la combinaison $a\xi + b\eta$, qui nous ont permis de définir d'une manière unique le calcul de deux symboles ξ et η qui satisfont aux relations

$$f(\xi) = 0, \qquad g(\eta) = 0.$$

Il est possible de substituer à ces relations (I) un autre système plus simple à certains points de vue, auquel nous allons parvenir en traitant l'une des questions posées dans un chapitre antérieur relativement au problème dont nous venons de nous occuper ; nous voulons parler de la *recherche de la réductibilité dans le domaine* $[\xi]$, dont nous rappelons ici l'objet :

On suppose que l'on ajoute à l'ensemble des nombres entiers un nombre algébrique entier ξ, qui vérifie la relation irréductible d'ordre m : $f(\xi) = 0$; on demande de fixer ensuite le caractère de toute équation irréductible à coefficients entiers $g(y) = 0$, au point de vue de la décomposition de son premier membre dans le domaine algébrique $[\xi]$.

Formons pour cela le résolvant $\text{R}(z, u, v)$ du système

$$(\text{I}) \qquad \begin{cases} f(x) = 0, \\ g(y) = 0, \end{cases}$$

et décomposons ce résolvant en ses facteurs irréductibles

$$\text{P}_i(z, u, v),$$

que nous supposerons en nombre égal à h. On a établi que ces facteurs sont essentiellement distincts et que le système (I) se *décompose* en h systèmes définis soit par une des identités en u et v :

$$\text{P}_i(ux + vy, u, v) = 0$$
$$(i = 1, 2, \ldots, h),$$

soit par les relations

$$\text{P}_i(z, a, b) = 0,$$
$$x\text{D}_z\text{P}_i(z, a, b) + \text{D}_a\text{P}_i(z, a, b) = 0,$$
$$y\text{D}_z\text{P}_i(z, a, b) + \text{D}_b\text{P}_i(z, a, b) = 0,$$

soit enfin par les relations

$$\text{P}_i(z, a, b) = 0,$$
$$f(x) = 0, \quad g(y) = 0.$$

Considérons maintenant les deux polynomes en y, $P_i(ax+by, a, b)$ et $g(y)$; nous pouvons exécuter sur ces polynomes les opérations qui conduisent au plus grand commun diviseur et, si nous désignons par $F(x)$ le dernier reste, il suffit d'observer que la relation

$$F(x) = 0$$

est compatible avec la relation $f(x) = 0$ pour en conclure que $F(x)$ est divisible par $f(x)$. On est ainsi conduit à trois identités de la forme

$$P_i(ax+by, a, b) = \alpha_i d_i(x, y) + A_i f(x),$$
$$g(y) = \beta_i d_i(x, y) + B_i f(x),$$
$$d_i(x, y) = \lambda_i P_i(ax+by, a, b) + \mu_i g(y) + \nu_i f(x),$$

où l'on désigne par α_i, β_i, A_i, B_i, λ_i, μ_i, ν_i des polynomes entiers en x et y à coefficients entiers. Nous dirons que le polynome $d_i(x, y)$, qui est le dernier diviseur employé, est *le plus grand commun diviseur de* $P_i(ax+by, a, b)$ *et de* $g(y)$ *suivant le module* $f(x)$, et nous entendons par là uniquement qu'on regarde comme nuls les multiples de $f(x)$.

Considérons les identités en x et y qu'on vient d'écrire ; on en déduit immédiatement, en tenant compte des propriétés du résolvant :

$$\prod d_i(x, y) = M(x, y).g(y) + N(x, y).f(x)$$

et

$$g(y) = m(x, y).\prod d_i(x, y) + n(x, y).f(x),$$

en désignant par M, N, m, n des polynomes entiers à coefficients entiers ; d'où l'on peut conclure en négligeant les multiples de $f(x)$, c'est-à-dire en remplaçant x par un nombre algébrique ξ qui vérifie la relation $f(\xi) = 0$,

$$M(\xi, y).m(\xi, y) = 1.$$

Il suffit alors d'observer que dans le domaine $[\xi]$ toutes les fonctions entières à coefficients entiers de ξ dont le degré est inférieur au degré du polynome $f(x)$, sont *des symboles distincts* dont un seul est nul, pour conclure de là les *identités en* y :

$$M(\xi, y) = 1 \qquad \text{et} \qquad m(\xi, y) = 1.$$

On a donc l'identité en x et en y :

$$g(y) = \prod d_i(x, y) + n(x, y).f(x),$$

d'où il résulte que nous savons former une décomposition du polynome $g(y)$ dans le domaine d'intégrité $[\xi]$, défini par la relation $f(\xi) = 0$.

Nous ajouterons que la manière dont nous avons obtenu les polynomes $d_i(x, y)$ montre que les relations

$$d_i(\xi, y) = 0 \qquad \text{et} \qquad d_k(\xi, y) = 0$$

sont incompatibles, c'est-à-dire que les divers polynomes $d_i(x, y)$ sont différents. Il est clair en outre qu'il n'existe aucune décomposition de la forme

$$d_i(\xi, y) = d'_i(\xi, y) . d''(\xi, y),$$

d'_i et d''_i désignant des polynomes à coefficients entiers, sans quoi le système

$$f(x) = 0, \qquad d_i(x, y) = 0$$

ne serait pas irréductible.

Il est donc légitime de dire que *la décomposition donnée du polynome $g(y)$ dans le domaine ξ est une décomposition en facteurs irréductibles.*

Nous ferons enfin remarquer que *cette décomposition est unique.*

Si nous avons en effet l'identité

$$g(y) = \prod e_k(x, y) + p(x, y) . f(x),$$

on en conclut que la relation $e_k(x, y) = 0$, où l'on peut supposer que x figure à un degré inférieur à celui de $f(x)$, est compatible avec les relations $f(x) = 0$ et $g(y) = 0$, d'où il résulte qu'elle est une conséquence nécessaire des relations de l'un des systèmes

$$d_i(x, y) = 0,$$
$$f(x) = 0$$

et une combinaison linéaire de ces relations. Admettons en outre qu'elle soit irréductible, c'est-à-dire qu'il n'existe aucune identité de la forme

$$e_k(x, y) = e'_k(x, y) . e''_k(x, y) + q(x, y) . f(x) ;$$

nous pourrons en conclure que le système

$$f(x) = 0,$$
$$e_k(x, y) = 0$$

est irréductible, et par conséquent que $d_i(x, y)$ est également une combinaison linéaire des relations de ce système.

Le raisonnement employé tout à l'heure montre alors qu'on a nécessairement

$$e_k(x, y) = d_i(x, y),$$

d'où résulte l'existence d'une seule décomposition de $g(y)$ en facteurs irréductibles dans le domaine $[\xi]$.

L'analyse précédente permettrait de remplacer l'adjonction au domaine $[\xi]$ d'un entier algébrique η vérifiant la relation $g(\eta) = 0$ par celle d'un entier algébrique vérifiant une des relations

$$d_i(\xi, \eta) = 0,$$

et l'on serait alors assuré, quand le degré de $d_i(\xi, \eta)$ par rapport à η surpasse l'unité, de la nécessité d'introduire le symbole η, alors qu'il peut arriver en procédant comme on l'a fait plus haut que le domaine $[\xi, \eta]$ se réduise effectivement au domaine $[\xi]$; mais il est préférable de raisonner symétriquement sur les symboles ξ et η et de rapporter toujours leur définition à l'ensemble des nombres entiers.

Le problème que nous venons de traiter a néanmoins une grande importance dans d'autres théories, telles que celle de la divisibilité des entiers algébriques dans le domaine $[\xi]$; comme nous n'avons pas l'intention de parler ici de cette question, nous renverrons le lecteur aux beaux travaux de Kronecker et de M. Dedekind sur ce sujet.

Ajoutons cependant que les deux relations

$$f(x) = 0, \qquad d_i(x, y) = 0$$

peuvent remplacer les trois relations

$$P_i(ax + by, a, b) = 0,$$
$$f(x) = 0, \qquad g(y) = 0,$$

par lesquelles nous avons défini le calcul des symboles ξ et η, et que ces deux systèmes sont liés de telle sorte que toute relation de l'un d'eux est une combinaison linéaire des relations de l'autre. Ces deux relations constituent la forme particulière des équations de définition de ξ et de η que nous avions annoncée plus haut.

II. — 2e MÉTHODE : **Résolvante de Galois.**

52. Il a été établi dans les pages qui précèdent que le calcul dans un domaine algébrique est déterminé d'une manière unique et com-

plètement connu, lorsqu'on sait constituer ce domaine par des adjonctions successives d'un seul symbole à un domaine dans lequel le calcul est déjà connu. Il ne se présente d'ailleurs dans ce calcul aucune contradiction.

Nous allons montrer qu'il en est de même dans le cas où *l'on ajoute simultanément, à un domaine dans lequel le calcul est déjà connu, tous les symboles distincts qui possèdent les modes de composition que nous avons imposés aux entiers algébriques et qui vérifient en outre la relation*

$$f(x) = 0,$$

où l'on désigne par $f(x)$ le polynome irréductible à coefficients entiers

$$x^n - p_1 x^{n-1} + \cdots \pm p_n.$$

Nous avons déjà établi qu'il ne peut exister plus de n symboles distincts $\xi_1, \xi_2, \dots, \xi_n$ possédant ces propriétés et que ces symboles, mis respectivement à la place de $x_1, x_2, \dots, x_n$, devront nécessairement vérifier les relations

$$S_1 = p_1, \qquad S_2 = p_2, \qquad \dots, \qquad S_n = p_n,$$

où l'on a désigné par $S_1, S_2, \dots, S_n$ les fonctions symétriques élémentaires des x.

On sait enfin que, réciproquement, lorsque ces dernières relations sont vérifiées, les symboles $x_1, x_2, \dots, x_n$ vérifient tous la relation

$$f(x) = 0$$

et sont, *à l'ordre près*, identiques aux symboles $\xi_1, \xi_2, \dots, \xi_n$.

Il reste donc à établir que les relations

$$\text{(A)} \qquad S_1 = p_1, \qquad S_2 = p_2, \qquad \dots, \qquad S_n = p_n$$

ne sont pas incompatibles et à montrer qu'elles suffisent pour déterminer le calcul des symboles $x_1, x_2, \dots, x_n$.

Nous observerons d'abord que si le système (A) possède des solutions, ces solutions sont *déterminées*, car tout élément x_i de l'une d'entre elles devant vérifier la relation $f(x_i) = 0$ ne peut être choisi d'une façon arbitraire dans un ensemble de symboles connus, parmi les nombres entiers par exemple.

Cela étant acquis, la symétrie des équations (A) nous montre que lorsque les égalités

$$x_1 = \xi_1, \qquad x_2 = \xi_2, \qquad \dots, \qquad x_n = \xi_n$$

définissent une solution de ces équations, il en sera de même des égalités

$$x_1 = \xi_{r_1}, \qquad x_2 = \xi_{r_2}, \qquad \dots, \qquad x_n = \xi_{r_n},$$

où l'on a désigné par $r_1, r_2, \dots, r_n$ les entiers $1, 2, \dots, n$, pris dans un mode arbitraire de succession.

La suite $r_1, r_2, \dots, r_n$ est dite former une *permutation* des entiers $1, 2, \dots, n$, et il est facile d'établir qu'il existe un nombre de permutations *distinctes*, c'est-à-dire différant au moins par les places occupées par deux entiers, égal au produit $1 . 2 . \dots . n$, produit qu'on écrit simplement $n\,!$.

Nous concluons de là que lorsque le système (A) admet une solution, il en admet certainement $n\,!$; sa résolvante générale est donc au moins de degré $n\,!$, et il suffit d'observer que d'autre part le degré de cette résolvante ne peut dépasser le produit des dimensions maxima des premiers membres des relations (A) pour en conclure qu'il est précisément égal à $n\,!$.

Considérons maintenant le produit

$$\prod (z - u_1 x_{r_1} - u_2 x_{r_2} - \cdots - u_n x_{r_n})$$

étendu à toutes les permutations $r_1, r_2, \dots, r_n$ des entiers $1, 2, \dots, n$; il est clair que ce produit est une fonction symétrique des x, car ses facteurs ne font que s'échanger lorsqu'on échange x_i et x_k. Nous savons donc l'exprimer et cela d'une manière seulement à l'aide des expressions $S_1, S_2, \dots, S_n$:

$$\prod (z - u_1 x_{r_1} - u_2 x_{r_2} - \cdots - u_n x_{r_n}) = F(z, S_1, S_2, \cdots, S_n).$$

Envisageons alors l'identité bien connue de Taylor :

$$F(z, S_1, S_2, \dots, S_n) = F(z, p_1, p_2, \dots, p_n)$$
$$+ \Sigma (S_i - p_i) D_{p_i} F(z, p_1, p_2, \dots, p_n) + \cdots ;$$

elle nous montre, lorsqu'on y remplace z par l'expression

$$u_1 x_1 + u_2 x_2 + \cdots + u_n x_n,$$

auquel cas on a identiquement par rapport aux x :

$$F(z, S_1, S_2, \dots, S_n) = 0,$$

que la relation $\qquad F(z, p_1, p_2, \dots, p_n) = 0$

est une conséquence nécessaire des relations

(A) $\qquad S_1 = p_1, \qquad S_2 = p_2, \qquad \dots, \qquad S_n = p_n$

et une combinaison linéaire de ces relations. Nous pouvons donc affirmer que *cette relation*

$$F(z, p_1, p_2, \dots, p_n) = 0$$

est la résolvante générale du système (A), et nous établissons ainsi que cette résolvante renferme effectivement z, c'est-à-dire que *les relations* (A) *ne sont jamais incompatibles.*

53. Il est facile de montrer que *la résolvante*

$$F(z, p_1, p_2, \dots, p_n) = 0$$

n'a pas de diviseurs multiples, lorsque les u *sont indéterminés.* Considérant pour cela le polynome

$$F(z, S_1, S_2, \dots, S_n) = \prod (z - u_1 x_{r_1} - u_2 x_{r_2} - \cdots - u_n x_{r_n})$$

et rappelant que le discriminant de ce polynome est le produit

$$\prod [u_1(x_{r_1} - x_{s_1}) + u_2(x_{r_2} - x_{s_2}) + \cdots + u_n(x_{r_n} - x_{s_n})]$$

étendu aux $n!\,(n! - 1)$ combinaisons deux à deux des $n!$ expressions

$$u_1 x_{r_1} + u_2 x_{r_2} + \cdots + u_n x_{r_n},$$

nous formerons dans ce discriminant, qui est homogène en $u_1, u_2, \dots, u_n$, le coefficient d'un terme que nous définissons de la manière suivante : prenons parmi tous les termes du discriminant tous ceux qui contiennent u_1 à l'ordre le plus élevé où il figure dans ce discriminant, puis parmi ceux-là tous ceux qui renferment u_2 à l'ordre le plus élevé, et ainsi de suite.

Il est clair que l'on parvient ainsi à un terme bien déterminé et qui ne peut être obtenu dans le produit précédent que d'une seule manière ; le coefficient de ce terme est donc un produit de différences $(x_i - x_k)$, et la symétrie du polynome exige que chacune de ces différences y figure le même nombre de fois. On conclut de là que le coefficient du terme considéré est une puissance du discriminant du produit

$$(x - x_1)(x - x_2)\dots(x - x_n),$$

c'est-à-dire du polynome

$$x^n - S_1 x^{n-1} + S_2 x^{n-2} - \cdots \pm S_n.$$

Il suffit maintenant d'observer que l'on passe de

$$F(z, S_1, S_2, \dots, S_n)$$

au résolvant $F(z, p_1, p_2, \ldots, p_n)$ en remplaçant simplement S_i par p_i, pour conclure de là que le coefficient du terme considéré dans le discriminant du résolvant est une puissance du discriminant Δ_f du polynome $f(x)$.

On peut donc dire que *si le polynome $f(x)$ est sans diviseurs multiples*, le discriminant du polynome $F(z, p_1, p_2, \ldots, p_n)$, qui est homogène en $u_1, u_2, \ldots, u_n$, ne sera pas identiquement nul et par suite que ce polynome sera aussi sans diviseurs multiples, lorsque les u sont indéterminés.

54. Ces résultats étant acquis, rien n'est plus facile que de définir des symboles distincts $\xi_1, \xi_2, \ldots, \xi_n$ qui vérifient la relation

$$f(x) = 0$$

et de montrer comment on déterminera le calcul de leurs fonctions entières. Désignons à cet effet par $R(z, u)$ le résolvant

$$F(z, p_1, p_2, \ldots p_n)$$

considéré comme fonction des z et des u, et par $G(z, u)$ l'un de ses diviseurs irréductibles lorsque les u demeurent indéterminés ; nous savons que si les entiers $a_1, a_2, \ldots, a_n$ sont choisis de telle sorte que le polynome $R(z, a)$ n'ait point de diviseurs multiples, le polynome $G(z, a)$ sera irréductible. Il suffira donc d'ajouter à l'ensemble des nombres entiers un symbole ζ assujetti à posséder les modes de composition imposés aux ξ et à vérifier la relation

$$G(\zeta, a) = 0,$$

pour obtenir à l'aide des relations

$$\xi_i D_\zeta G(\zeta, a) + D_{a_i} G(\zeta, a) = 0$$

$$(i = 1, 2, \ldots, n)$$

l'expression explicite de n symboles $\xi_1, \xi_2, \ldots, \xi_n$ qui possèdent les modes de composition exigés et vérifient les relations (A). Ces symboles sont nécessairement distincts, car ils vérifient l'identité

$$f(x) = (x - \xi_1)(x - \xi_2)\ldots(x - \xi_n)$$

et nous savons que le discriminant de $f(x)$, qui est alors identique au produit $\prod(\xi_i - \xi_k)$, est différent de zéro.

Si l'on observe d'autre part que l'on a

$$\zeta = a_1\xi_1 + a_2\xi_2 + \cdots + a_n\xi_n,$$

ainsi qu'il résulte de l'homogénéité du polynome $G(z, a_1, a_2, \ldots, a_n)$.

on en conclut que le domaine algébrique $[\xi_1, \xi_2, \ldots, \xi_n]$ est identique au domaine constitué par le seul entier algébrique ζ, c'est-à-dire au domaine $[\zeta]$. Il résulte de là que dans ce domaine $[\xi_1, \xi_2, \ldots, \xi_n]$, le calcul est déterminé d'une manière unique, complètement connu et qu'il ne renferme point de contradiction.

55. Il convient de répondre immédiatement à une question que suggèrent les remarques précédentes : Lorsque le résolvant $R(z, u)$ est irréductible, il n'existe qu'une seule manière de définir ζ, car la relation $R(z, a) = 0$, conséquence nécessaire des relations (A), est irréductible ; le calcul des entiers $\xi_1, \xi_2, \ldots, \xi_n$ est donc déterminé d'une manière unique par la définition que nous avons donnée de ces entiers, et la méthode que nous employons pour les définir à l'aide de ζ est *nécessaire*. Qu'arrive-t-il lorsque ce résolvant admettant des diviseurs $G_k(z, u)$, nécessairement distincts, le procédé que nous venons d'indiquer conduit à des définitions distinctes du symbole ζ, suivant que l'on part de l'un ou de l'autre des diviseurs irréductibles du résolvant ?

Nous observerons d'abord que la relation $R(z, a) = 0$, qui est une conséquence nécessaire des relations (A), entraine nécessairement l'une des relations $G_k(z, a) = 0$ et que cette dernière exclut toutes les autres relations de cette forme. Si l'on ajoute que les équations

$$R(z, a) = 0,$$

$$x_i D_z R(z, a) + D_{a_i} R(z, a) = 0$$

$$(i = 1, 2, \ldots, n)$$

forment un système équivalent aux relations (A), il sera clair qu'on ne peut déduire des relations (A) aucune raison pour égaler à zéro l'un des facteurs irréductibles de $R(z, a)$ de préférence à un autre. Il est donc nécessaire d'égaler à zéro l'un de ces facteurs *choisi d'une manière arbitraire*, et la relation ainsi obtenue compatible avec les relations (A) n'est pas une combinaison linéaire de ces relations.

Supposons qu'on ait défini ζ par la relation $G(\zeta, a) = 0$; nous pouvons prévoir aisément le changement produit lorsqu'on remplace ζ par le symbole ζ_k défini par la relation

$$G_k(\zeta_k, a) = 0.$$

Nous savons en effet que si l'on a

$$\xi_i D_\zeta G(\zeta, a) + D_{a_i} G(\zeta, a) = 0$$
$$(i = 1, 2, \ldots, n),$$

toutes les solutions du système (A) sont obtenues et obtenues une seule fois en écrivant

$$x_1 = \xi_{r_1}, \qquad x_2 = \xi_{r_2}, \qquad \ldots \qquad x_n = \xi_{r_n},$$

où l'on désigne par $r_1, r_2, \ldots, r_n$ l'une quelconque des $n!$ permutations des entiers $1, 2, \ldots, n$. Si l'on considère par conséquent les symboles $\tau_1, \tau_2, \ldots, \tau_n$ définis par les relations

$$\tau_i D_{\zeta_k} G_k(\zeta_k, a) + D_{a_i} G_k(\zeta_k, a) = 0$$
$$(i = 1, 2, \ldots, n),$$

ces symboles sont simplement les entiers algébriques $\xi_1, \xi_2, \ldots, \xi_n$ rangés dans autre ordre. Supposons par exemple $\tau_i = \xi_{k_i}$, la suite $k_1, k_2, \ldots, k_n$ désignant une certaine permutation des entiers 1, 2, ..., n ; la substitution de $G_k(z, a)$ à $G(z, a)$ équivaut uniquement à appeler ξ_i l'entier algébrique désigné par ξ_{k_i} dans la première hypothèse.

Fixer le facteur irréductible de $R(z, a)$, c'est donc préciser dans une certaine mesure la notation des entiers algébriques $\xi_1, \xi_2, \ldots, \xi_n$, d'où il résulte qu'il est légitime de dire que les relations (A) permettent dans tous les cas de définir d'une manière unique le calcul de symboles $\xi_1, \xi_2, \ldots, \xi_n$ qui vérifient ces relations ou bien l'identité en x

$$f(x) = (x - \xi_1)(x - \xi_2)\ldots(x - \xi_n).$$

56. L'équation irréductible $G(z, a) = 0$ dont ζ est par définition l'une des racines, a été considérée en premier lieu par Galois qui en a fait le fondement de sa théorie des équations ; nous l'appellerons suivant l'usage, *résolvante de Galois* de l'équation $f(x) = 0$. Signalons-en ici une propriété importante, sur laquelle nous reviendrons d'ailleurs plus tard : *tous les entiers algébriques qui vérifient la relation* $G(z, a) = 0$ *sont des fonctions entières à coefficients entiers d'un quelconque d'entre eux.*

Nous venons de voir en effet que si l'on désigne par ζ l'un de ces entiers algébriques, les relations

$$\xi_i D_\zeta G(\zeta, a) + D_{a_i} G(\zeta, a) = 0$$
$$(i = 1, 2, \ldots, n)$$

donnent l'expression des ξ comme fonctions entières à coefficients entiers de ζ. Si l'on observe que toutes les solutions de la résolvante générale $R(z, a) = 0$ s'obtiennent en écrivant

$$z = a_1\xi_{r_1} + a_2\xi_{r_2} + \cdots + a_n\xi_{r_n},$$

$r_1, r_2, \ldots, r_n$ désignant une permutation quelconque des entiers $1, 2, \ldots, n$, ainsi qu'il résulte de la façon dont nous avons obtenu cette résolvante ou encore de la symétrie des relations (A), on en conclut que *tous les entiers algébriques qui vérifient la relation* $R(z, a) = 0$ *sont des fonctions entières à coefficients entiers de* ζ, ce qui comprend en particulier la propriété annoncée de l'équation $G(z, a) = 0$.

Il importe également d'attirer l'attention sur une conséquence immédiate de l'analyse précédente. Appelons *équation normale* toute équation irréductible à coefficients entiers qui possède la propriété qu'on vient d'établir pour la résolvante de Galois, autrement dit toute équation telle que tous les entiers algébriques qui la vérifient soient des fonctions entières à coefficients entiers de l'un d'entre eux ; appelons également *entier algébrique normal* tout entier algébrique qui vérifie une équation normale ; on pourra énoncer la proposition suivante :

Tout entier algébrique est fonction entière à coefficients entiers d'un entier algébrique normal; d'où l'on conclut qu'*on devra chercher parmi les entiers algébriques normaux, les symboles-types qu'il est nécessaire d'introduire dans le calcul pour que toute équation irréductible à coefficients entiers ait un nombre de racines distinctes égal à son degré.*

57. Revenons maintenant au sujet de nos recherches, qui consiste à définir le calcul des entiers algébriques dans tout domaine que l'on peut constituer en ajoutant simultanément à un domaine dans lequel le calcul est déjà connu, tous les entiers algébriques qui vérifient une même équation irréductible à coefficients entiers.

Nous avons montré comment peut se faire la première adjonction, l'équation dont on adjoint les racines étant $f(x) = 0$, et nous avons établi par là la possibilité de définir logiquement n racines de cette équation. Considérons le domaine $[\zeta]$ ainsi obtenu et proposons-nous d'adjoindre à ce domaine les p racines de l'équation irréductible de degré p à coefficients entiers : $g(y) = 0$. Nous savons que cette opération équivaut à l'adjonction au domaine ζ

d'un seul entier algébrique θ, défini par une relation irréductible à coefficients entiers :

$$H(\theta, b) = 0,$$

que nous avons d'ailleurs appris à former. On est donc amené à définir le calcul dans le domaine algébrique $[\zeta, \theta]$, les symboles ζ et θ étant assujettis à vérifier les relations irréductibles à coefficients entiers

$$G(\zeta, a) = 0,$$
$$H(\theta, b) = 0.$$

C'est là un problème que nous avons résolu au début de ce chapitre. On y a établi que le domaine $[\zeta, \theta]$ est identique à un domaine $[\varphi]$ formé par l'adjonction d'un seul entier algébrique φ, défini par une équation irréductible à coefficients entiers que l'on sait former, entier algébrique qui est d'ailleurs de la forme $u_0\zeta + v_0\theta$, u_0 et v_0 étant deux entiers ordinaires ; d'où il résulte que le calcul est déterminé dans ce domaine et ne renferme point de contradiction.

Il convient d'observer en passant que lorsque le résolvant du système

$$G(z, a) = 0,$$
$$H(t, b) = 0$$

est irréductible, on est amené à préciser la racine de la seconde équation que l'on désignera par θ et qu'on adjoint au domaine $[\zeta]$, c'est-à-dire à préciser encore la définition de chacun des entiers algébriques $\eta_1, \eta_2, \ldots, \eta_p$ qui vérifient la relation $g(y) = 0$, en tenant compte de la manière dont ils se comportent vis-à-vis d'une racine ζ de $G(z, a) = 0$.

Nous ferons également sur l'entier algébrique φ que nous venons de considérer une remarque importante. Il résulte de la propriété des résolvantes de Galois signalée tout à l'heure, que si l'on a

$$G(\zeta, a) = 0,$$
$$H(\theta, b) = 0,$$

on peut également écrire les identités en z et en t :

$$G(z, a) = \prod [z - \lambda_i(\zeta)],$$

$$H(t, b) = \prod [t - \mu_k(\theta)],$$

en désignant respectivement par $\lambda_i(\zeta)$ et $\mu_k(\theta)$ des polynomes entiers à coefficients entiers en ζ et en θ, tels que l'on ait

$$\lambda_1(\zeta) = \zeta, \qquad \mu_1(\theta) = \theta,$$

et qui représentent tous les nombres algébriques entiers qui vérifient les deux relations

$$G(z, a) = 0,$$
$$H(t, b) = 0.$$

On conclut de là que le résolvant du système formé par ces deux relations est décomposable en facteurs linéaires de la forme

$$uz + vt - u\lambda_i(\zeta) - v\mu_k(\theta),$$

et par conséquent que si ζ et θ sont des fonctions entières à coefficients entiers de l'entier algébrique φ, défini par la relation

$$\varphi = u_0\zeta + v_0\theta,$$

toutes les autres racines de l'équation résolvante qui sont les expressions $u_0\lambda_i(\zeta) + v_0\mu_k(\theta)$ sont également des fonctions entières à coefficients entiers de φ. *L'entier algébrique φ est par conséquent un entier algébrique normal,* et la méthode que nous employons pour définir le calcul dans un domaine que l'on sait former en ajoutant simultanément, à un domaine formé de même, tous les entiers algébriques qui vérifient une même équation irréductible à coefficients entiers, ne conduit à ajouter à l'ensemble des entiers ordinaires que des entiers algébriques normaux.

Tout domaine de cette nature s'obtient donc en ajoutant à l'ensemble des nombres entiers, un seul entier algébrique normal convenablement choisi, d'où il résulte que le calcul y est défini d'une manière unique et ne renferme aucune contradiction.

58. Il convient de faire immédiatement, sur ce calcul, quelques observations importantes qu'on développera plus loin d'une manière complète.

Considérons le domaine $[\xi_1, \xi_2, \ldots, \xi_n]$ formé par les entiers algébriques $\xi_1, \xi_2, \ldots, \xi_n$ que nous avons définis par les relations

$$G(\zeta, a) = 0,$$
$$\xi_i D_\zeta G(\zeta, a) + D_{a_i} G(\zeta, a) = 0$$
$$(i = 1, 2, \ldots, n);$$

nous savons que si l'on désigne par α le degré du polynome $G(z, a)$, les polynomes à coefficients entiers de degré inférieur à α

$$\lambda_1(\zeta) = \zeta, \qquad \lambda_2(\zeta), \qquad \ldots, \qquad \lambda_\alpha(\zeta)$$

représentent tous les entiers algébriques qui vérifient la relation $G(\zeta, a) = 0$; proposons-nous de rechercher quel est l'effet de la substitution à ζ d'une autre racine $\zeta_k = \lambda_k(\zeta)$ de la résolvante de Galois sur la définition des symboles $\xi_1, \xi_2, \ldots, \xi_n$ et sur le calcul de leurs fonctions entières à coefficients entiers.

On sait *a priori* que les entiers algébriques $\xi_1^{\zeta_k}, \xi_2^{\zeta_k}, \ldots, \xi_n^{\zeta_k}$ définis par les relations

$$\xi_i^{\zeta_k} D_{\zeta_k} G(\zeta_k, a) + D_{a_i} G(\zeta_k, a) = 0$$
$$(i = 1, 2, \ldots, n)$$

sont simplement les entiers algébriques $\xi_1, \xi_2, \ldots, \xi_n$ rangés dans un ordre convenable, si l'on a par exemple

$$\xi_i^{\zeta_k} = \xi_{k_i},$$

en désignant par $k_1, k_2, \ldots, k_n$ une permutation déterminée des entiers $1, 2, \ldots, n$, la substitution de ζ_k à ζ équivaut à appeler ξ_i l'entier algébrique appelé ξ_{k_i} dans la première hypothèse (*). En d'autres termes, aux diverses racines $\zeta_1 = \zeta, \zeta_2, \ldots, \zeta_\alpha$ de la résolvante de Galois correspondent diverses permutations des éléments $\xi_1, \xi_2, \ldots, \xi_n$ qu'on peut désigner par $P_1, P_2, \ldots, P_\alpha$, et la substitution de ζ_k à ζ remplace les éléments de P_k par les éléments de même rang dans P_1.

Nous observerons également que le calcul des fonctions entières à coefficients entiers de $\xi_1, \xi_2, \ldots, \xi_n$, qui est déterminé d'une manière unique par la définition qu'on a donnée de ces symboles à l'aide de ζ, est nécessairement identique au calcul des fonctions entières des symboles $\xi_1^{\zeta_k}, \xi_2^{\zeta_k}, \ldots, \xi_n^{\zeta_k}$, qui sont définis de la même manière à l'aide de ζ_k. Cela résulte immédiatement de ce que toutes les relations entières à coefficients entiers en ζ restent vraies pour ζ_k, ou encore de ce que les deux calculs dont on vient de parler se déduisent uniquement des relations identiques

$$G(\zeta, a) = 0,$$
$$G(\zeta_k, a) = 0.$$

(*) Il est bien évident qu'on ne peut avoir pour toute valeur de i $\xi_i = \xi_{k_i}$, puisque ζ et ζ_k sont distincts et liés aux ξ par les relations

$$\zeta = a_1\xi_1 + \cdots + a_n\xi_n, \qquad \zeta_k = a_1\xi_{k_1} + \cdots + a_n\xi_{k_n};$$

la substitution de ζ_k à ξ produit donc véritablement un changement dans la définition des ξ.

On conclut de là que si l'on considère par exemple une relation entière à coefficients entiers

$$F(\xi_1, \xi_2, \ldots, \xi_n) = 0,$$

elle reste vraie lorsqu'on y remplace respectivement $\xi_1, \xi_2, \ldots, \xi_n$ par $\xi_{k_1}, \xi_{k_2}, \ldots, \xi_{k_n}$ et cela quel que soit k. *Il existe donc dans le calcul des fonctions entières de* $\xi_1, \xi_2, \ldots, \xi_n$ *une certaine symétrie définie par les permutations*

$$P_1, P_2, \ldots, P_\alpha,$$

symétrie que nous nous bornons à reconnaître ici et que nous étudierons de plus près dans la suite.

59. Nous avons étudié dans les pages qui précèdent la constitution des domaines algébriques par des adjonctions successives de l'une des racines d'une équation irréductible à coefficients entiers ou de toutes les racines d'une équation de cette nature. Il est facile de montrer que tous les domaines algébriques s'obtiennent nécessairement par l'un ou l'autre de ces procédés.

Considérons en effet un système irréductible *quelconque* de relations entières à coefficients entiers entre des symboles

$$x_1, x_2, \ldots, x_n;$$

nous désignerons par $R(z, u)$ sa résolvante générale que l'on supposera renfermer z, le coefficient de la plus haute puissance de z étant l'unité.

Nous savons qu'alors on peut substituer au système donné les relations

$$R(z, u) = 0,$$

$$x_i D_z R(z, u) + D_{u_i} R(z, u) = 0$$

$$(i = 1, 2, \ldots, n),$$

où z désigne la combinaison

$$u_1 x_1 + u_2 x_2 + \ldots + u_n x_n.$$

Il résulte de là que si les a sont choisis de telle sorte que le polynome $R(z, a)$ n'ait point de diviseurs multiples, le système considéré aura autant de solutions dans un domaine quelconque que l'équation $R(z, a) = 0$ y a de racines.

En particulier, si l'on ajoute à l'ensemble des entiers un des entiers algébriques qui vérifient la relation irréductible

$$R(\zeta, a) = 0,$$

le système donné sera vérifié par les entiers algébriques

$$\xi_1, \xi_2, \ldots, \xi_n$$

définis par les relations

$$\xi_i D_\zeta R(\zeta, a) + D_{a_i} R(\zeta, a) = 0$$
$$(i = 1, 2, \ldots, n).$$

On pourra donc exprimer d'une manière explicite les éléments de toutes les solutions du système en introduisant dans le calcul toutes les racines de l'équation irréductible à coefficients entiers

$$R(z, a) = 0,$$

et le nombre de ces solutions distinctes est précisément le degré de cette résolvante générale.

Il convient enfin d'observer que le domaine algébrique défini par les éléments de toutes ces solutions est simplement le domaine formé en ajoutant aux entiers l'une des racines de la résolvante de Galois de l'équation $R(z, a) = 0$; c'est donc un domaine algébrique *normal*, c'est-à-dire un domaine constitué par l'adjonction aux entiers d'un entier algébrique normal.

III. — Équations spéciales, leur groupe.

60. La définition que nous avons donnée des racines

$$\xi_1, \xi_2, \ldots, \xi_n$$

de l'équation $f(x) = 0$, à l'aide d'une racine ζ de la résolvante de Galois

$$G(z, a) = 0,$$

conduit de la manière la plus naturelle à une classification des équations irréductibles, que nous allons maintenant présenter.

Examinons d'abord une équation $f(x) = 0$ pour laquelle le système

$$\text{(A)} \qquad S_1 = p_1, \quad S_2 = p_2, \ldots, \quad S_n = p_n$$

est irréductible, c'est-à-dire pour laquelle la résolvante générale de ce système : $R(z, u_1, u_2, \ldots, u_n) = 0$ est irréductible lorsque les u sont indéterminés. On a vu que la résolvante de Galois est alors

$$R(z, a_1, a_2, \ldots, a_n) = 0\,;$$

on observe qu'elle est de degré $n!$, d'où il résulte qu'en rempla-

çant ζ par une quelconque de ses racines, on peut remplacer les éléments de la suite $\xi_1, \xi_2, \ldots, \xi_n$ par les éléments de même rang dans une permutation quelconque.

Toute relation entière en $\xi_1, \xi_2, \ldots, \xi_n$ à coefficients entiers demeure donc vraie lorsqu'on y remplace respectivement

$$\xi_1, \xi_2, \ldots, \xi_n$$

par les éléments correspondants $\xi_{k_1}, \xi_{k_2}, \ldots, \xi_{k_n}$ d'une permutation quelconque P_k.

C'est d'ailleurs ce que l'on peut conclure aussi d'une propriété des systèmes irréductibles signalée antérieurement : Toute relation entière en $x_1, x_2, \ldots, x_n$ à coefficients entiers, compatible avec les relations (A), est une combinaison linéaire de ces relations.

Il résulte de là que si l'on considère le domaine $[\xi_1, \xi_2, \ldots, \xi_n]$ comme constitué par les fonctions entières de $\xi_1, \xi_2, \ldots, \xi_n$ à coefficients entiers qui sont de degré au plus égal à $n-i$ par rapport à ξ_i, aucun des éléments ainsi obtenus, si ce n'est zéro lui-même, ne peut être nul ; tous ces éléments doivent donc être regardés comme des symboles distincts, et la forme que nous leur donnons permet de trouver et de représenter sans ambiguïté la somme et le produit de deux d'entre eux.

Les équations irréductibles à coefficients entiers qui possèdent la propriété précédente, c'est-à-dire pour lesquelles le système

$$\text{(A)} \qquad S_1 = p_1, \qquad S_2 = p_2, \qquad \ldots, \qquad S_n = p_n$$

est irréductible, sont dites *générales* ; les autres sont appelées *spéciales*, c'est de ces dernières que nous allons maintenant nous occuper.

Nous supposons par conséquent le résolvant $R(z, u_1, u_2, \ldots, u_n)$ du système (A) *réductible lorsque les u demeurent indéterminés* et nous désignons par $G_1(z, u)$, $G_2(z, u)$, ..., $G_\varsigma(z, u)$ ses divers diviseurs irréductibles. On sait qu'alors la résolvante de Galois est toute équation $G_1(z, a) = 0$, dans laquelle les a sont choisis de telle sorte que le polynome en z qui en forme le premier membre n'ait pas de diviseurs multiples. Admettons qu'on ait choisi d'une manière arbitraire la relation

$$G_1(\zeta, a) = 0$$

pour définir ζ et par suite les entiers algébriques $\xi_1, \xi_2, \ldots, \xi_n$

par les formules

$$\xi_i D_\zeta G_1(\zeta, a) + D_{a_i} G_1(\zeta, a) = 0\ ;$$

nous rappelons que si α désigne le degré du polynome $G_1(z, a)$ et si les polynomes

$$\lambda_1(\zeta) = \zeta, \qquad \lambda_2(\zeta), \qquad \dots, \qquad \lambda_\alpha(\zeta)$$

représentent les divers entiers algébriques qui vérifient l'équation

$$G_1(z, a) = 0,$$

la substitution de $\lambda_k(\zeta)$ à ζ dans la définition des ξ équivaut à remplacer ξ_i par le symbole ξ_{k_i} qui occupe le même rang dans une permutation convenable P_k des ξ. Nous avons déjà fait observer que cette substitution de $\lambda_k(\zeta)$ à ζ ne change en rien le calcul dans le domaine $[\zeta]$, d'où il résulte que *toute relation entière en* ξ_1, $\xi_2, \dots, \xi_n$ *à coefficients entiers demeure vraie lorsqu'on y remplace respectivement par les éléments* $\xi_1, \xi_2 \dots, \xi_n$ *de la permutation* P_1 *les éléments de même rang* $\xi_{k_1}, \xi_{k_2}, \dots, \xi_{k_n}$ *de toute permutation* P_k *qui appartient à la suite* $P_1, P_2, \dots, P_\alpha$.

On peut aussi parvenir à cette proposition de la manière suivante : Considérons l'équation $G_1(z, a) = 0$ où z représente la combinaison $a_1x_1 + a_2x_2 + \dots + a_nx_n$ et qui définit quand on l'ajoute aux relations (A) l'un des systèmes irréductibles en lesquels le système (A) se décompose. Nous savons que

$$\lambda_1(\zeta) = a_1\xi_1 + \cdots + a_n\xi_n$$

et

$$\lambda_k(\zeta) = a_1\xi_{k_1} + \cdots + a_n\xi_{k_n}$$

sont deux racines de cette équation, il en résulte que les égalités :

$$x_1 = \xi_1, \qquad x_2 = \xi_2, \qquad \dots \qquad x_n = \xi_n,$$

$$x_1 = \xi_{k_1}, \qquad x_2 = \xi_{k_2}, \qquad \dots, \qquad x_n = \xi_{k_n}$$

définissent deux solutions du système irréductible considéré. Si l'on observe que la première d'entre elles est également définie par les égalités

$$x_{k_1} = \xi_{k_1}, \qquad x_{k_2} = \xi_{k_2}, \qquad \dots, \qquad x_{k_n} = \xi_{k_n},$$

on pourra en conclure que le système irréductible dont la résolvante générale est

$$G_1(u_1x_{k_1} + u_2x_{k_2} + \cdots + u_nx_{k_n}, u) = 0$$

admet une solution du système irréductible dont la résolvante générale est

$$G_1(u_1x_1 + u_2x_2 + \cdots + u_nx_n, u) = 0,$$

et par suite que ces deux systèmes sont identiques.

L'ensemble des équations qui définissent le système irréductible considéré demeure par conséquent le même lorsqu'on remplace respectivement par $x_1, x_2, \ldots, x_n$ les éléments de même rang x_{k_1}, $x_{k_2}, \ldots, x_{k_n}$ de la permutation P_k des x.

On conclut de là que toute relation

$$G_1(a_1x_{k_1} + a_2x_{k_2} + \cdots + a_nx_{k_n}, a) = 0$$

est une combinaison linéaire des $(n+1)$ relations :

$$S_1 = p_1, \qquad S_2 = p_2, \qquad \ldots, \qquad S_n = p_n,$$
$$G_1(a_1x_1 + a_2x_2 + \cdots + a_nx_n, a) = 0,$$

qui définissent le système irréductible considéré, ce qui établit la proposition annoncée plus haut.

61. Il convient d'appeler ici l'attention sur une propriété remarquable du système des permutations $P_1, P_2, \ldots, P_\alpha$.

Nous savons que si

$$\zeta = a_1\xi_1 + a_2\xi_2 + \ldots + a_i\xi_i$$

désigne l'une des racines de la résolvante de Galois $G_1(z, a) = 0$, toutes les racines de cette équation sont

$$\lambda_1(\zeta) = \zeta, \qquad \lambda_2(\zeta), \qquad \ldots, \qquad \lambda_\alpha(\zeta).$$

Il résulte de là que la suite des polynomes

$$\lambda_1[\lambda_k(\zeta)], \qquad \lambda_2[\lambda_k(\zeta)], \qquad \ldots, \qquad \lambda_\alpha[\lambda_k(\zeta)].$$

que nous écrirons plus simplement

$$\lambda_1(\lambda_k), \qquad \lambda_2(\lambda_k), \qquad \ldots, \qquad \lambda_\alpha(\lambda_k),$$

représente également toutes ces racines ; cette suite est donc une simple permutation des éléments $\lambda_1, \lambda_2, \ldots, \lambda_\alpha$. Admettons que l'on ait par exemple

$$\lambda_i(\lambda_k) = \lambda_{(i,k)},$$

en désignant par (i, k) un entier convenablement choisi dans la suite $1, 2, \ldots, \alpha$; l'opération précédente remplacera respectivement les éléments $\lambda_1, \lambda_2, \ldots, \lambda_\alpha$ par les éléments de même rang dans la suite $\lambda_{(1,k)}, \lambda_{(2,k)}, \ldots, \lambda_{(\alpha,k)}$.

D'autre part, substituer $\lambda_k(\zeta)$ à ζ équivaut à remplacer par les éléments de P_1 les éléments correspondants de P_k ; on peut

donc dire que *cette opération remplace d'une manière générale par les éléments de* P_i *les éléments correspondants de* $P_{(i,k)}$, *c'est-à-dire remplace par les permutations*

$$P_1, \quad P_2, \quad \ldots, \quad P_\alpha$$

les permutations de même rang dans la suite

$$P_{(1,k)}, \quad P_{(2,k)}, \quad \ldots, \quad P_{(\alpha,k)},$$

qui est composée des mêmes permutations. En d'autres termes, *le système des permutations* $P_1, P_2, \ldots, P_\alpha$ *se reproduit lorsqu'on y effectue sur les* ξ *le changement qui conduit de* P_k *à* P_1, *et le changement qu'éprouvent les* P *est inverse de celui qu'éprouvent les racines* $\lambda(\zeta)$ *de la résolvante de Galois.*

A toute équation spéciale correspond donc un système de permutations de n lettres $\xi_1, \xi_2, \ldots, \xi_n$ parmi lesquelles figure P_1 et qui possède la propriété précédente ; nous verrons tout à l'heure comment on a fondé sur cette remarque la classification des équations spéciales. Pour l'instant nous nous bornerons à signaler encore la propriété suivante du système des permutations $P_1, P_2, \ldots, P_\alpha$: On a vu que lorsque

$$u_1\xi_1 + u_2\xi_2 + \cdot \cdot + u_n\xi_n$$

représente l'une des racines de l'équation

$$G_1(z, u_1, u_2, \ldots, u_n) = 0,$$

il en est de même de $u_1\xi_{k_1} + u_2\xi_{k_2} + \cdots + u_n\xi_{k_n}$; il suffit d'observer qu'on peut écrire la première expression sous la forme

$$u_{k_1}\xi_{k_1} + u_{k_2}\xi_{k_2} + \cdots + u_{k_n}\xi_{k_n}$$

pour en conclure que l'on passe de la seconde à la première en remplaçant respectivement par $u_1, u_2, \ldots, u_n$ les éléments u_{k_1}, $u_{k_2}, \ldots, u_{k_n}$.

Le polynome $G_1(z, u_1, u_2, \ldots, u_n)$ *demeure par suite invariable lorsqu'on effectue sur les* u le *changement qui conduit de* P_k *à* P_1 en désignant par P_k l'une quelconque des permutations $P_1, P_2, \ldots, P_\alpha$.

Nous venons de constater de diverses manières l'existence dans le calcul des fonctions entières à coefficients entiers de

$$\xi_1, \xi_2, \ldots, \xi_n,$$

d'une certaine symétrie définie par les permutations

$$P_1, P_2, \ldots, P_\alpha ;$$

il est facile de montrer qu'il n'existe pas d'autres changements des ξ qui transforment en elles-mêmes les tables d'addition et de multiplication de leurs fonctions entières. Nous allons y parvenir en faisant voir comment tous les systèmes irréductibles qui correspondent à l'équation donnée dérivent de l'un d'entre eux, par exemple de celui que nous avons choisi.

Désignons à cet effet par

$$u_1\xi_{r_1} + u_2\xi_{r_2} + \ldots + u_n\xi_{r_n}$$

l'une des racines de la résolvante

$$G_r(z, u_1, u_2, \ldots, u_n) = 0,$$

et considérons l'expression $u_{r1}\xi_{r_1} + u_{r2}\xi_{r_2} + \ldots + u_{rn}\xi_{r_n}$ qui représente une racine de l'équation

$$G_1(z, u_1, u_2, \ldots, u_n) = 0.$$

Il est clair que l'équation

$$G_r(z, u_{r_1}, u_{r_2}, \ldots, u_{r_n}) = 0$$

admet l'une des racines de l'équation précédente ; on en conclut que leurs premiers membres sont identiques.

Les diverses résolvantes dérivent donc de l'une d'entre elles

$$G_1(z, u_1, u_2, \ldots, u_n) = 0$$

en y remplaçant respectivement les éléments $u_{r_1}, u_{r_2}, \ldots, u_{r_n}$ d'une permutation convenable des u, par $u_1, u_2, \ldots, u_n$. Elles son par suite de même degré en z, et si nous désignons par β leur nombre, on a

$$\alpha\beta = n\,!.$$

Il suffit d'observer que le système irréductible de relations entre $x_1, x_2, \ldots, x_n$ déduit de l'identité

$$G_r(u_1x_1 + \ldots + u_nx_n, \quad u_1, \ldots, u_n) = 0$$

dérive de celui qu'on a adopté pour définir les ξ, c'est-à-dire de celui qui correspond à l'identité

$$G_1(u_1x_1 + \ldots + u_nx_n, \quad u_1, \ldots, u_n) = 0,$$

en remplaçant dans ce dernier les éléments $x_1, x_2, \ldots, x_n$ par les éléments $x_{r_1}, x_{r_2}, \ldots, x_{r_n}$, pour en conclure que la même opération effectuée sur les ξ conduit à de nouvelles tables de calcul *incompatibles* avec les premières. Les seuls changements qui n'altèrent pas les tables d'addition et de multiplication des fonctions en-

tières à coefficients entiers de $\xi_1, \xi_2, \ldots, \xi_n$ sont donc ceux qui conduisent de P_1 à P_k, lorsque P_k fait partie de la suite

$$P_1, P_2, \ldots, P_\nu.$$

62. Les résultats précédents sont susceptibles de prendre une forme très élégante par l'introduction et l'emploi systématique d'une notion dont nous avons fait jusqu'à présent un usage constant, sans toutefois la mettre en évidence, notion que nous allons maintenant présenter. Étant données n lettres $a_1, a_2, \ldots, a_n$, on appelle *substitution* de ces n lettres l'opération qui consiste à remplacer respectivement $a_1, a_2, \ldots, a_n$ par $a_{r_1}, a_{r_2}, \ldots, a_{r_n}$, où l'on désigne par $r_1, r_2, \ldots, r_n$ une permutation quelconque des entiers $1, 2, \ldots, n$. Une substitution est donc complètement définie lorsqu'on donne avec chacun des entiers de la suite $1, 2, \ldots, n$ celui par lequel on le remplace, et il est clair que le nombre des substitutions différentes est égal à $n!$ lorsqu'on y comprend l'opération qui n'altère aucun de ces entiers et qu'on appelle *substitution identique*. Nous ferons remarquer en outre qu'à toute substitution qui remplace l'entier i par l'entier r_i correspond la substitution qui remplace r_i par i et qui est dite l'*inverse* de la première.

Les propriétés les plus importantes des opérations que nous venons de définir dérivent de l'existence d'un mode de composition de ces opérations entre elles, qui possède des propriétés extrêmement simples : désignons par la lettre unique s la substitution qui remplace d'une manière générale l'entier i par l'entier s_i et par t la substitution qui remplace de même l'entier i par l'entier t_i ; cette dernière opération remplacera l'entier s_i par un certain entier que nous désignons d'une manière générale par u_i, et il est clair que la substitution u qui remplace directement l'entier i par u_i produit le même changement que les substitutions s et t effectuées l'une à la suite de l'autre et dans l'ordre indiqué. Cette substitution u est le résultat d'une composition des substitutions s et t, à laquelle, en raison de ses propriétés, on a donné le nom de *multiplication* (*) ;

(*) On verra bientôt que ces propriétés sembleraient légitimer tout aussi bien l'emploi du nom addition, mais nous ajouterons immédiatement que dans d'autres parties des mathématiques, on considère simultanément le mode précédent et un autre mode qui possède alors les propriétés de l'addition des entiers.

la substitution u est alors appelée *produit* de s par t; s est le *multiplicande*, t le *multiplicateur*. Si nous convenons d'écrire

$$s.t = u,$$

nous pourrons définir le produit de trois substitutions en posant

$$r.s.t = (r.s).t,$$

$(r.s)$ désignant le produit de r par s; on reconnait immédiatement alors qu'on a aussi $r.s.t = r.(s.t)$, c'est-à-dire que *la composition considérée est associative*. En effet, la substitution $(r.s)$ remplace l'entier i par l'entier r_{s_i} et la substitution t remplace ce dernier par l'entier $r_{s_{t_i}}$ qui peut évidemment être obtenu aussi en remplaçant dans r_i l'indice i par s_{t_i}.

Nous ajouterons immédiatement que la *composition* dont il s'agit *n'est pas commutative*, c'est-à-dire qu'on n'a pas

$$s.t = t.s,$$

ainsi qu'il résulte de l'expression des entiers s_{t_i} et t_{s_i} que ces opérations substituent à l'entier i; c'est là une circonstance qui la distingue de la multiplication des entiers ordinaires et qui est la raison de la difficulté, et aussi d'ailleurs de l'intérêt, que présente l'étude des substitutions au point de vue où nous les envisageons.

Si l'on observe que la substitution identique peut être négligée dans un produit, soit comme multiplicande, soit comme multiplicateur, on pourra la représenter par l'unité, et comme d'autre part le produit d'une substitution s par la substitution inverse est toujours la substitution identique, on est conduit à désigner cette dernière par s^{-1} et à écrire

$$s.s^{-1} = 1.$$

Il résulte de là que les relations

$$s.t = u,$$
$$s'.t = u$$

entrainent nécessairement

$$s.t.t^{-1} = u.t^{-1},$$
$$s'.t.t^{-1} = u.t^{-1},$$

d'où l'on conclut : $s = s'$; on établirait de même que les relations analogues

$$s.t = u,$$
$$s.t' = u$$

exigent
$$t = t'.$$

Les remarques qui précèdent, jointes à ce fait que le produit $s.t$ est différent de s et de t lorsqu'aucun de ces facteurs n'est l'unité, établissent donc que *si l'on considère des substitutions distinctes et si on les multiplie, soit à droite, soit à gauche, par une même substitution on obtient encore des substitutions distinctes.*

En résumé, lorsqu'on envisage au point de vue de leur composition par une multiplication les n ! substitutions distinctes de n lettres, les symboles qui les représentent se manifestent comme possédant les propriétés suivantes :

1° *De deux symboles quelconques du système, on peut déduire d'une manière déterminée un troisième symbole du même système ;*

2° *La composition considérée est associative ;*

3° *Un même symbole composé avec des symboles différents donne des symboles différents.*

Nous reconnaissons là les propriétés qui, dans un chapitre antérieur, nous ont servi à définir un *groupe* ; les n ! substitutions de n lettres constituent donc un groupe limité lorsqu'on les compose entre elles par multiplication ; ce groupe est appelé *groupe symétrique* de n lettres et va jouer dans la suite un rôle important.

Si l'on se reporte maintenant aux résultats énoncés naguère à l'aide des permutations des entiers $1, 2, \ldots, n$, on verra immédiatement que tous ces résultats peuvent s'exprimer de la manière suivante :

Soient : $f(x) = 0$ *une équation spéciale d'ordre* n,

$$\xi_1, \xi_2, \ldots, \xi_n$$

les racines de cette équation, définies en partant d'une racine ξ *de la résolvante de Galois :*

$$G_1(z, a_1, a_2, \ldots, a_n) = 0,$$

dont l'ordre est α,

il existe un groupe de substitutions des n *lettres* ξ, *formé de* α *substitutions et tels que :*

Toute substitution de ce groupe laisse invariable l'ensemble des relations entières à coefficients entiers entre $\xi_1, \xi_2, \ldots, \xi_n$, *ou toute portion de cet ensemble qui le détermine nécessairement. Toute substitution n'appartenant pas au groupe substitue à cet ensemble un autre ensemble de relations incompatibles avec les premières.*

Si l'on considère les diverses résolvantes partielles en nombre β :

$$G_1(z, u_1, u_2, \ldots, u_n) = 0, \ldots, G_\beta(z, u) = 0$$

toute substitution du même groupe effectuée sur les u, laisse invariable chacun des polynomes G ; *toute autre substitution échange entre eux ces divers polynomes.*

Ajoutons qu'il résulte de là que le *groupe de l'équation* est complètement déterminé, soit par la relation entière entre les ξ :

$$G_1(a_1\xi_1 + a_2\xi_2 + \ldots + a_n\xi_n,\ a_1,\ a_2,\ \ldots,\ a_n) = 0,$$

soit par le polynome entier en u :

$$G_1(z,\ u_1,\ u_2,\ \ldots,\ u_n).$$

Ces résultats étant acquis, on a rangé dans une même *classe* toutes les équations irréductibles d'ordre n, qui conduisent au même groupe, et il est clair que la classification ainsi obtenue est naturelle, nous dirons même *nécessaire*, puisque les relations qui lient aux entiers les racines de deux équations d'une même classe ne diffèrent jamais que par le nom de ces racines et les déterminations des coefficients et que cette circonstance cesse de se produire lorsqu'on passe d'une classe à une autre.

63. Il convient avant d'aborder d'une façon systématique l'étude des groupes de substitutions, de présenter encore quelques remarques générales au sujet des groupes limités et des rapports qui existent entre ces groupes et les groupes de substitutions.

Considérons un groupe limité d'objets bien définis (p. 133) et appelons, pour fixer les idées, *multiplication*, la composition de nature déterminée que l'on sait effectuer sur ces objets ou éléments.

Nous observons d'abord qu'*il existe toujours un élément qui, multiplié par un élément donné soit à droite, soit à gauche, conduit à un produit donné.*

Soient, en effet, $a, b, \ldots l$ les divers éléments du groupe, i l'un quelconque d'entre eux ; les produits

$$ai,\ bi,\ \ldots li$$

sont tous différents ; ils font d'ailleurs partie du groupe, ce sont donc dans un autre ordre les éléments $a, b, \ldots l$, et l'un d'entre eux, ki par exemple, est identique à l'élément i.

On établirait de même que dans la suite $ia,\ ib,\ \ldots,\ il$ l'un des produits ik' est aussi identique à i.

Les égalités

$$ki = i,$$
$$ik' = i$$

montrent que d'une part l'élément k est négligeable dans la multiplication à gauche *par* i et l'élément k' négligeable dans la multiplication à droite *par* i.

Je dis que ceci a lieu pour tous les éléments, mis à la place de i; il suffit en effet d'appliquer la propriété associative de la multiplication pour écrire, par exemple :

$$ia = (ki)a = k(ia),$$

ce qui démontre la proposition pour l'élément ia, qui est quelconque lorsque a est quelconque.

Enfin si l'on fait en particulier $i = k'$ et $i = k$ dans les deux identités

$$ki = i,$$
$$ik' = i,$$

on en déduit $kk' = k' = k$, c'est-à-dire que les éléments k et k' sont identiques.

Désignons par 1 cet élément qui est d'effet nul dans la multiplication ; nous venons de voir qu'il existe nécessairement un élément qui, multiplié à droite ou à gauche par un élément donné a, reproduit l'unité ; d'une manière plus précise, il existe deux éléments b et c tels que l'on ait

$$ab = 1, \qquad ca = 1.$$

Je dis que l'on a $b = c$; il suffit pour obtenir ce résultat de multiplier à gauche par c la première des égalités précédentes ; nous poserons $b = c = a^{-1}$ et nous dirons que a^{-1} est *l'inverse de* a.

On voit qu'il est possible de démontrer en partant de la définition d'un groupe limité quelconque, l'existence d'un élément unité et des éléments inverses ; nous allons compléter ces remarques en donnant la notion d'*isomorphisme*.

On dit que deux groupes sont *isomorphes* lorsqu'on peut établir entre les éléments de l'un et les éléments de l'autre une correspondance univoque et réciproque telle qu'au produit de deux éléments quelconques corresponde le produit des deux éléments correspondants pris dans le même ordre (*). En somme, au point de

(*) L'isomorphisme ainsi défini est dit *holoédrique*, par opposition à l'isomorphisme *mériédrique* que nous définirons plus loin.

vue abstrait auquel nous nous sommes placés jusqu'ici, les deux groupes sont *identiques* ou diffèrent tout au plus par les notations : c'est seulement lorsqu'on considère des groupes portant sur des objets bien déterminés que cette notion peut avoir de l'intérêt.

Nous allons montrer que *tout groupe limité est isomorphe à un groupe de substitutions* ; nous pourrons donc nous borner à étudier les groupes de substitutions, et toutes les propositions que nous établirons ainsi et dans l'*énoncé* desquelles ne figurera pas explicitement la nature des éléments du groupe, s'appliqueront aux groupes limités quelconques.

La démonstration de la proposition énoncée est d'ailleurs immédiate : nous pouvons toujours désigner les éléments du groupe donné, supposés en nombre n, par une même lettre a, affectée des indices 1, 2, 3, ..., n. Écrivons ces éléments sur une même ligne :

$$a_1, \ a_2, \ a_3, \ \dots, \ a_n,$$

et écrivons au-dessous leurs produits par un élément quelconque a_i ; soient

$$a_{i_1}, \ a_{i_2}, \ a_{i_3}, \ \dots, \ a_{i_n}$$

ces produits. Désignons par s_i la substitution qui remplace les indices 1, 2, 3, ..., n par les indices i_1, i_2, ..., i_n, qui ne diffèrent des premiers que par l'ordre. Il est clair que les substitutions s_i forment un groupe isomorphe au groupe des a_i ; en effet, la substitution s_i remplace l'indice α par l'indice α_i lorsque le produit de a_α par a_i est a_{α_i} ; on peut dire que l'effet de la substitution s_i sur les indices considérés pour eux-mêmes est identique à l'effet de la multiplication par a_i sur les indices considérés comme faisant corps avec les a ; il est bien évident par suite que le produit de deux substitutions correspond de la même manière au produit des éléments correspondants.

Remarquons que le groupe de substitutions ainsi obtenu est de *degré n*, c'est-à-dire comporte n *indices*, et d'*ordre n*, c'est-à-dire renferme n substitutions. De plus, étant donnés deux indices quelconques i et k, il existe une substitution et une seule du groupe qui remplace i par k (en effet dans le groupe des a_i il y a un seul élément qui, multiplié par a_i, donne pour produit a_k ; c'est ce que l'on exprime en disant que le groupe de substitutions est *simplement transitif*. Ainsi *tout groupe limité d'ordre n est isomorphe à un*

groupe transitif de substitutions entre n *lettres, dont l'ordre est aussi égal à* n. Un tel groupe est appelé *groupe normal* et la raison de cette dénomination apparait immédiatement lorsqu'on observe que le groupe de toute équation normale irréductible est nécessairement de cette espèce. Si en particulier nous considérons la résolvante de Galois $G_1(z, a) = 0$, dont les racines sont :

$$\lambda_1(\zeta) = \zeta, \qquad \lambda_2(\zeta), \ldots, \lambda_\alpha(\zeta)$$

nous savons que les transformations entières

$$[z, \lambda_1(z)], \qquad [z, \lambda_2(z)], \ldots, [z, \lambda_\alpha(z)]$$

envisagées suivant le module $G_1(z, a)$, constituent un groupe limité dont l'ordre est égal à α ; ce groupe est d'ailleurs isomorphe avec le groupe de l'équation $f(x) = 0$ ainsi qu'il l'a été établi par la considération des permutations

$$P_1, P_2, \ldots, P_\alpha$$

qui définissent ce dernier groupe et qui correspondent d'une manière univoque et réciproque avec les $\lambda_i(\zeta)$.

Ajoutons enfin que la proposition précédente s'applique en particulier aux groupes de substitutions dont l'ordre n'est pas égal au degré et qu'elle sera pour nous d'une grande importance dans ce cas particulier.

CHAPITRE V

LES GROUPES DE SUBSTITUTIONS

I. — Structure des substitutions.

64. Nous avons, dans le précédent chapitre, défini les substitutions et leur multiplication ; nous avons également montré comment on peut, à l'aide des $n!$ permutations, former toutes les substitutions distinctes de n lettres, mais nous n'avons donné jusqu'à présent aucune indication générale sur la manière dont chaque substitution échange entre elles les lettres $x_1, x_2, \ldots, x_n$, c'est-à-dire sur la *structure* des substitutions : il est aisé de combler cette lacune.

Considérons une substitution quelconque et soit a_1 un indice pris au hasard dans la suite $1, 2, \ldots, n$; la substitution remplacera cet indice par un autre, que nous appellerons a_2; elle remplacera de même a_2 par a_3, et ainsi de suite. Mais comme le nombre des indices est limité, on arrivera sûrement ainsi, avant n opérations, à un indice a_h que la substitution remplace par le premier indice a_1. Les termes de la suite $a_1, a_2, \ldots, a_h$ éprouvent par la substitution un changement très simple : si on les range, dans l'ordre où on les trouve, sur un cercle décrit dans un sens déterminé, on peut dire que chacun d'eux est remplacé par le suivant. Pour consacrer cette interprétation on donne le nom de *cycle* au système $a_1, a_2, \ldots, a_h$ et on dit que ces indices éprouvent une *substitution circulaire*.

Si le cycle comprend tous les indices, c'est-à-dire si $h = n$, on dit que la substitution considérée est *circulaire*.

Sinon, un indice étranger au cycle donne naissance à un nouveau

cycle, et ainsi de suite. Remarquons enfin qu'une lettre inaltérée par la substitution peut être regardée comme formant à elle seule un cycle.

Il résulte de là que *toute substitution de n lettres est circulaire ou se décompose en substitutions circulaires de moins de n lettres.* Enfin il est clair qu'une telle décomposition n'est possible que d'une seule manière et que deux cycles qui y figurent n'ont aucun indice commun.

Pour avoir une représentation de la substitution qui mette en évidence l'effet qu'elle produit, il faut donc donner les indices de chaque cycle ; on convient de représenter une substitution circulaire des indices $a_1, a_2, \ldots, a_h$ par le signe $(a_1, a_2, \ldots, a_h)$, la signification de ce signe ne changeant pas lorsqu'on commence par écrire l'une quelconque des lettres du cycle. Toute substitution pourra alors se représenter de la manière suivante :

$$(a_1, \ldots, a_h)(b_1, \ldots, b_k) \ldots,$$

en n'écrivant pas les cycles d'une seule lettre.

65. Deux substitutions sont dites *semblables* lorsqu'à chaque cycle de l'une correspond dans l'autre un cycle déplaçant le même nombre d'indices. Il est clair que deux substitutions semblables ne peuvent différer que par le nom des indices corrrespondants, c'est-à-dire par la notation ; on dit qu'elles appartiennent à un même *type*. On voit aisément qu'à toute décomposition du nombre n en entiers, de la forme

$$n = \alpha.h + \beta.k + \gamma.l + \ldots,$$

correspondent des substitutions de n lettres, formées de α cycles de h lettres, β cycles de k lettres, etc... ; le nombre des types distincts est donc celui des décompositions distinctes de n ayant cette forme. On observe que l'on pourra ranger les nombres $h, k, l, \ldots,$ qui sont nécessairement différents, dans leur ordre de grandeur, de façon que pour que deux décompositions de n soient distinctes, il faut et il suffit que deux des termes de même rang dans les deux décompositions soient différents.

Proposons-nous d'évaluer le nombre des substitutions de n lettres qui appartiennent à un type donné :

$$n = \alpha.h + \beta.k + \gamma.l + \ldots$$

Nous observerons que chaque substitution de ce type peut être écrite sous forme d'un produit de substitutions circulaires de

$$\alpha!h^\alpha.\beta!k^\beta.\gamma!l^\gamma\ldots$$

manières différentes : on peut en effet effectuer sur les cycles de h lettres une substitution quelconque et dans chacun d'eux une substitution circulaire, ce qui donne h manières distinctes d'écrire le cycle. Supprimons dans les expressions ainsi obtenues de chaque substitution du type donné, les parenthèses qui séparent les cycles; nous aurons des permutations des x, et il est facile de voir qu'on obtient ainsi toutes les permutations des x et chacune d'elles une seule fois. On conclut de là que *le nombre des substitutions des x qui appartiennent au type donné est égal au quotient de n ! par* $\alpha!h^\alpha.\beta!k^\beta.\gamma!l^\gamma\ldots$.

Ajoutons qu'on en déduit immédiatement l'identité arithmétique

$$\sum\frac{1}{\alpha!h^\alpha.\beta!k^\beta.\gamma!l^\gamma\ldots}=1,$$

où la somme qui figure au premier membre est étendue à toutes les décompositions :

$$n=\alpha.h+\beta.k+\gamma.l+\ldots.$$

66. Soit a une substitution quelconque des x; considérons la suite des puissances a, a^2, a^3, ... ; il est clair que les termes de cette suite ne peuvent être tous distincts puisque le nombre des substitutions différentes est limité; désignons par a^{m+1} le premier des termes de la suite qui reproduit l'un des précédents; on aura nécessairement

$$a^{m+1}=a,$$

car si l'on avait $a^{m+1}=a^{k+1}$, on en déduirait $a^{m-k+1}=a$, ce qui est contraire à l'hypothèse faite sur m. Il résulte de là que dans la suite a, a^2, a^3, ..., les mêmes substitutions se reproduisent de m en m, ou encore que a^m est d'effet nul dans la multiplication; a^m est donc la substitution identique. Les substitutions a, a^2, ..., $a^m=1$ forment un groupe d'ordre m, qu'on dit *dérivé* de la substitution a. Le nombre m est également appelé *ordre* de la substitution a.

Il est facile de voir qu'une substitution circulaire de p lettres est d'ordre p et il en résulte immédiatement que l'ordre d'une

substitution qui renferme des cycles de h, k, l, etc. lettres est le plus petit commun multiple des nombres h, k, l, etc.

La connaissance de l'ordre d'une substitution permet également quelquefois de trouver sa forme; par exemple toute substitution d'ordre premier p ne contient que des cycles de p lettres, et si elle contient seulement p lettres elle est circulaire.

II. — Fonctions rationnelles de n éléments.

67. Représentons par les lettres $x_1, x_2, \ldots, x_n$ des symboles distincts pour lesquels nous supposerons uniquement qu'ils se composent, entre eux et avec les entiers, suivant deux modes différents qui possèdent les propriétés fondamentales de l'addition et de la multiplication des entiers ordinaires; nous savons ainsi ce qu'on doit entendre par *fonctions rationnelles*, à coefficients entiers, de $x_1, x_2, \ldots, x_n$; nous nous proposons d'étudier ici les diverses espèces de symétrie que peuvent présenter ces fonctions ou, d'une manière plus précise, d'étudier comment elles se comportent lorsqu'on effectue sur les lettres x, les substitutions d'un groupe donné.

Nous ferons immédiatement observer, à ce sujet, que si l'on désigne par $p_1, p_2, \ldots, p_n$ les fonctions symétriques élémentaires des x, ces fonctions, ainsi que toutes leurs fonctions rationnelles à coefficients entiers, demeurent inaltérées par toute substitution faite sur les x, c'est-à-dire jouent, au point de vue où nous nous plaçons, le rôle d'éléments invariables. Il suffit alors de se reporter aux identités qui définissent $p_1, p_2, \ldots, p_n$ pour en conclure qu'à toute fonction rationnelle des x, correspond une fonction entière des mêmes lettres, dont le degré en x_i est au plus égal à $n-i$ et qui présente la même espèce de symétrie. Nous pourrons donc, dès que nous y trouverons un avantage quelconque, nous borner à considérer ces fonctions entières, ou d'une manière générale toutes les fonctions entières des x à coefficients entiers.

La question précédente est intimement liée à l'étude des groupes de substitutions et nous allons tout d'abord mettre cette liaison en évidence.

Si nous désignons par s une substitution quelconque des indices $1, 2, \ldots, n$ (ou des lettres $x_1, x_2, \ldots, x_n$, ce qui revient au

même), nous définirons la *transformée* d'une fonction entière φ des n lettres par la substitution s, comme la fonction obtenue en remplaçant dans φ chaque lettre par celle que la substitution s lui fait correspondre ; nous désignerons ce résultat par φs. Il est clair que *les substitutions qui laissent invariable une fonction entière de n lettres forment un groupe*, car si s et s' sont de telles substitutions, on a les identités

$$\varphi s = \varphi, \qquad \varphi s' = \varphi,$$

et par suite

$$\varphi\, ss' = \varphi s . s' = \varphi s' = \varphi,$$

c'est-à-dire que ss' laisse aussi invariable la fonction φ.

Réciproquement, *à tout groupe correspond une fonction φ qui est invariable par les substitutions de ce groupe et par celles-là seulement.*

Soient en effet $a, b, \ldots, l$ les substitutions distinctes du groupe considéré G. Nous avons signalé précédemment la fonction

$$V = m_1 x_1 + m_2 x_2 + \cdot \cdot + m_n x_n$$

qui prend par toutes les substitutions possibles $n\,!$ formes distinctes lorsque les entiers $m_1, m_2, \ldots, m_n$ sont convenablement choisis.

Désignons par $V_a, V_b, \ldots, V_l$ les résultats obtenus en effectuant sur V les substitutions de G. La suite $V_a, V_b, \ldots, V_l$ est seulement permutée par une substitution h du groupe G, car elle devient

$$V_{ah}, V_{bh}, \ldots, V_{lh},$$

et les substitutions $ah, bh, \ldots, lh$, toutes distinctes et appartenant à G, sont dans un autre ordre les substitutions $a, b, \ldots, l$.

Il résulte de là qu'une fonction symétrique quelconque de $V_a, V_b, \ldots, V_l$ demeure invariable par les substitutions de G. Il peut très bien arriver que, grâce à sa forme particulière, elle demeure aussi invariable par d'autres substitutions que celles de G, nous en verrons plus loin des exemples ; mais il est facile de former des fonctions qui varient par toute substitution n'appartenant pas à G.

Le produit $(A - V_a)(A - V_b) \ldots (A - V_l)$, où A est un élément invariable par toute substitution, par exemple un nombre entier, satisfait évidemment à cette condition. C'est en effet un polynome entier en $x_1, \ldots, x_n$, décomposable en facteurs linéaires rationnels ; nous savons que cette décomposition n'est possible que

d'une seule manière, si donc le produit demeure invariable par une substitution g, celle-ci ne peut qu'échanger entre eux les facteurs linéaires et par suite appartient à G.

Lorsqu'une fonction $\varphi(x_1, x_2, \ldots, x_n)$ demeure invariable par toutes les substitutions d'un groupe G, on dit qu'elle est un *invariant* du groupe. Si le groupe G est le plus grand groupe dont les substitutions laissent φ invariable, la fonction φ varie par toute autre substitution, on dit alors qu'elle est un *invariant caractéristique* du groupe. Le groupe des substitutions qui laissent invariable une fonction φ, pour lequel elle est évidemment un invariant caractéristique, est appelé *groupe de la fonction* φ.

Nous pourrons donc énoncer les résultats obtenus de la manière suivante :

Toute fonction de $x_1, x_2, \ldots, x_n$ *est un invariant caractéristique d'un certain groupe de substitutions entre ces lettres.*

Tout groupe de substitutions possède des invariants caractéristiques et l'on sait en former une infinité. Nous verrons plus tard qu'on peut les déduire tous d'un seul d'entre eux.

Les deux propositions précédentes nous permettent une classification des fonctions rationnelles de $x_1, x_2, \ldots, x_n$: il suffit de regarder comme fonctions d'un même *genre* tous les invariants caractéristiques d'un même groupe. Il est clair que tous les invariants caractéristiques d'un même groupe présentent par rapport à $x_1, x_2, \ldots, x_n$ la même espèce de symétrie ; on peut donc dire qu'il y a autant d'espèces de symétrie distinctes que de groupes de substitutions entre $x_1, x_2, \ldots, x_n$.

La question qui se pose maintenant est de construire effectivement la classification indiquée, c'est-à-dire de donner un type de chaque espèce de symétrie dont sont susceptibles les fonctions rationnelles de $x_1, x_2, \ldots, x_n$. Cette question exige la formation de tous les groupes de substitutions entre n lettres.

Si cette seconde question est résolue, nous savons en effet à l'aide d'une fonction qui varie par toute substitution former un invariant caractéristique de chaque groupe.

Le procédé indiqué à l'aide de la fonction linéaire

$$m_1x_1 + m_2x_2 + \ldots + m_nx_n$$

paraît peu commode dès que le groupe renferme un certain nombre

de substitutions distinctes, aussi nous allons en indiquer un autre qui donne toujours des fonctions de même degré en $x_1, x_2, \ldots, x_n$ et qui n'exige aucun calcul.

Considérons la fonction $x_1^{\alpha_1}.x_2^{\alpha_2}.\ \ldots\ x_n^{\alpha_n}$, où $\alpha_1, \alpha_2, \ldots \alpha_n$ sont des entiers distincts; il est clair que cette fonction varie par toute substitution. Si nous la désignons par V, la somme

$$V_a + V_b + \ldots\ldots + V_l$$

sera évidemment un invariant caractéristique pour le groupe G dont les substitutions distinctes sont $a, b, \ldots, l$. Cette somme est en effet un polynome en $x_1, x_2, \ldots, x_n$ formé d'autant de termes distincts qu'il y a de substitutions dans G, c'est-à-dire qu'il n'existe entre les différentes formes de V aucune réduction possible. De l'identité de deux valeurs de la somme $V_a + V_b + \ldots\ldots + V_l$ on peut donc conclure l'identité des divers termes et par suite le fait que la substitution qui laisse invariable la somme permute seulement ces termes entre eux. Donc elle appartient au groupe G.

En particulier, on peut prendre pour V la fonction $x_1x_2^2x_3^3\ \ldots\ x_{n-1}^{n-1}$, ainsi que l'a fait remarquer Kronecker.

Malheureusement, on ne sait pas jusqu'à présent former tous les groupes de substitutions de n lettres. Il est donc impossible de réaliser la classification indiquée et nous devrons nous borner à étudier les groupes et les fonctions rationnelles particulières qu'il nous sera utile de connaître.

Remarquons d'ailleurs qu'il n'est pas nécessaire de construire effectivement la classification précédente pour être édifié sur sa valeur; il suffit d'approfondir les rapports qui existent d'une part entre deux fonctions de genres différents, d'autre part entre deux fonctions du même genre. C'est ce que nous ferons dans le chapitre suivant.

Parmi les fonctions rationnelles de $x_1, x_2, \ldots, x_n$, les plus simples sont les fonctions symétriques qui sont des invariants pour un groupe quelconque et des invariants caractéristiques pour le groupe formé de toutes les substitutions possibles. Ce groupe, qui est évidemment composé symétriquement avec les lettres $x_1, x_2, \ldots, x_n$, est appelé *groupe symétrique*. Tous les autres groupes sont formés d'un certain nombre de substitutions de ce dernier; on dit qu'ils

sont des *sous-groupes* du groupe symétrique; nous signalerons seulement ici le plus grand de ces groupes, pour lequel la fonction

$$\delta = (x_1 - x_2) \ldots (x_1 - x_n)(x_2 - x_3) \ldots (x_{n-1} - x_n)$$

est un invariant caractéristique. On sait que le carré de δ est une fonction symétrique des x que nous avons appelée *discriminant* du produit $(x - x_1) \ldots (x - x_n)$; il en résulte qu'une substitution quelconque faite sur les x ne peut que changer le signe de δ et l'on voit par exemple que la substitution (x_{n-1}, x_n) change effectivement ce signe. Les $n!$ substitutions se partagent donc en deux classes suivant qu'elles changent ou non le signe de δ, et il est clair que les deux classes comportent le même nombre de substitutions.

Le groupe de $\frac{n!}{2}$ substitutions ainsi obtenu est appelé *groupe alterné* des n lettres; nous établirons plus loin quelques-unes de ses propriétés les plus importantes.

III. — Propriétés générales des groupes.

68. Soit $\varphi(x_1, x_2, \ldots, x_n)$ une fonction non symétrique des x; désignons par p l'ordre de son groupe G, par $a, b, \ldots, l$ ses substitutions distinctes.

On a la suite d'identités

$$\varphi a = \varphi b = \ldots\ldots = \varphi l;$$

si donc s est une substitution n'appartenant pas à G, on a aussi

$$\varphi as = \varphi bs = \ldots\ldots = \varphi ls;$$

les substitutions $as, bs, \ldots, ls$ sont distinctes entre elles et aussi distinctes des précédentes, car $as = b$ donne $s = a^{-1}b$ et s appartiendrait à G. Soit de même t une substitution nouvelle

$$\varphi at = \varphi bt = \ldots\ldots = \varphi lt,$$

et l'on n'a pas $at = bs$, car on en déduirait $t = a^{-1}b.s$.

En continuant ainsi on voit que la fonction φ prend $\frac{n!}{p}$ formes distinctes par toutes les substitutions possibles.

Le nombre des formes distinctes que peut prendre une fonction rationnelle des x est donc toujours un diviseur de $n\,!$, ou autrement : *l'ordre d'un groupe quelconque est un diviseur de* $n\,!$.

Il s'en faut de beaucoup que la réciproque de cette proposition soit exacte, c'est-à-dire qu'à tout diviseur p de $n\,!$ corresponde un groupe d'ordre p.

On peut, par exemple, démontrer que, n étant plus grand que 4, si une fonction de $x_1, x_2, \ldots, x_n$ a plus de deux formes elle en a au moins n, ce qui exclut l'existence de fonctions à moins de n formes autres que les fonctions symétriques et les fonctions à deux formes. On trouvera dans le savant ouvrage de M. Jordan (*) une foule d'autres propositions particulières. Nous ne donnerons pas ici ces développements qui ne seraient pour nous d'aucune utilité ; nous nous bornons à dire qu'on ne sait pas encore les conditions nécessaires et suffisantes que doit remplir un nombre p pour qu'il existe des groupes d'ordre p formés de substitutions de n lettres.

Rappelons qu'un groupe H est dit sous-groupe d'un groupe donné G lorsque toutes les substitutions de H appartiennent à G.

Désignons par p l'ordre de G, par q l'ordre de H et par $h_1 = 1$, $h_2, \ldots, h_q$ les substitutions distinctes de H.

Si g_2 est une substitution de G n'appartenant pas à H, G renfermera également les substitutions

$$g_2h_1, \qquad g_2h_2, \qquad \ldots, \qquad g_2h_q.$$

Ces q substitutions sont distinctes ; elles sont d'ailleurs différentes des précédentes, car d'une égalité

$$g_2h_\alpha = h_\beta$$

on pourrait déduire

$$g_2 = h_\beta h_\alpha^{-1},$$

ce qui est contraire à l'hypothèse faite sur g_2. Donc G renferme au moins $2q$ substitutions distinctes.

Supposons qu'il en renferme davantage ; soit g_3 l'une de celles qui n'ont pas encore été obtenues, G renfermera également les q substitutions distinctes

$$g_3h_1, \qquad g_3h_2, \qquad \ldots, \qquad g_3h_q$$

(*) C. Jordan : *Traité des Substitutions et des équations algébriques*, Gauthier-Villars, 1870.

qui n'appartiennent pas à H, comme on vient de le montrer pour g_2. Je dis que ces substitutions sont également différentes des substitutions g_2h. Si on avait en effet

$$g_3h_\alpha = g_2h_\beta,$$

on en déduirait

$$g_3 = g_2h_\beta h_\alpha^{-1},$$

et g_3 appartiendrait à la seconde suite. Donc G renferme au moins $3q$ substitutions distinctes.

En continuant ce raisonnement on épuisera certainement les p substitutions de G, et si l'on désigne par λ le nombre des substitutions g dont on s'est servi, y compris la substitution

$$g_1 = 1$$

qui donne le groupe H, on peut écrire l'égalité $p = \lambda . q$, qui prouve que :

Si H *est un sous-groupe de* G, *l'ordre de* H *est un diviseur de l'ordre de* G.

L'analyse précédente montre que les p substitutions de G peuvent être rangées dans le tableau suivant :

$$\begin{array}{cccc} h_1 = 1 & h_2 & \dots & h_q \\ g_2 & g_2h_2 & \dots & g_2h_q \\ \dots & \dots & \dots & \dots \\ g_\lambda & g_\lambda h_2 & \dots & g_\lambda h_q. \end{array}$$

Il est bien évident qu'on aurait pu les obtenir également en multipliant à droite les substitutions de H par des substitutions g. On a donc également le tableau

$$\begin{array}{cccc} h_1 = 1 & h_2 & \dots & h_q \\ g_2 & h_2g_2 & \dots & h_qg_2 \\ \dots & \dots & \dots & \dots \\ g_\lambda & h_2g_\lambda & \dots & h_qg_\lambda, \end{array}$$

où nous avons laissé les mêmes lettres g pour ne pas multiplier les notations, mais où ces lettres ne désignent pas nécessairement les mêmes substitutions. Lorsqu'on choisit l'un des modes de génération, il ne reste plus d'arbitraire que la place de chaque élément dans sa ligne et l'ordre de ces lignes, autrement dit : *l'ensemble de tous les éléments d'une ligne demeure le même.*

En effet, toute substitution de G n'appartenant pas à H peut s'écrire $g_\beta h_\alpha$, et si on la multiplie à droite par les éléments de H on obtient des résultats de la forme $g_\beta h_\alpha h$, qui sont évidemment tous les éléments de la ligne g_β et ceux-là seulement.

Le nombre λ introduit par l'égalité $p = \lambda . q$ s'appelle l'*indice* du sous-groupe H dans le groupe G. L'importance de ce nombre ressort clairement du théorème suivant :

Tout invariant caractéristique de H *prend* λ *formes distinctes lorsqu'on lui applique toutes les substitutions du groupe* G.

Soit en effet Φ un invariant caractéristique de H, c'est-à-dire une fonction qui demeure invariable par les substitutions de H et par celles-là seulement ; si h désigne une substitution quelconque de H, on a l'identité

$$\Phi h = \Phi.$$

Transformons les deux membres par une des substitutions $g_2, g_3, \ldots, g_\lambda$, par exemple g_α; nous obtiendrons la nouvelle identité

$$\Phi h g_\alpha = \Phi g_\alpha ,$$

c'est-à-dire que toutes les substitutions de la ligne qui contient g_α transformeront Φ en une même fonction Φg_α.

Toutes les fonctions ainsi obtenues sont distinctes, car d'une relation

$$\Phi g_\alpha = \Phi g_\beta$$

on déduirait $\Phi g_\alpha . g_\beta^{-1} = \Phi$, c'est-à-dire $g_\alpha . g_\beta^{-1} = h$ ou enfin $g_\alpha = h g_\beta$, ce qui est contraire à l'hypothèse faite sur les g.

Donc aux substitutions $hg_1 = h$, $hg_2, \ldots hg_\lambda$, où h est une substitution quelconque de H pouvant être différente dans hg_i et hg_k par exemple, correspondent λ formes distinctes de Φ : $\Phi g_1, \Phi g_2, \ldots, \Phi g_\lambda$, que nous désignerons simplement par

$$\Phi = \Phi_1, \qquad \Phi_2, \qquad \ldots, \qquad \Phi_\lambda.$$

Ces fonctions sont dites *conjuguées dans le groupe* G.

69. Nous savons d'après les théorèmes fondamentaux établis au début de ce chapitre que $\Phi_2, \Phi_3, \ldots, \Phi_\lambda$ sont les invariants caractéristiques de certains groupes bien déterminés. Quels sont ces groupes et quels rapports ont-ils avec le groupe H de la fonction $\Phi_1 = \Phi$?

Considérons l'une des fonctions précédentes, Φ_α par exemple, soit k une substitution qui n'altère pas Φ_α ; on aura

$$\Phi g_\alpha k = \Phi g_\alpha,$$

et l'on en déduit en transformant par la substitution g_α^{-1} :

$$\Phi g_\alpha k g_\alpha^{-1} = \Phi.$$

La substitution $g_\alpha k g_\alpha^{-1}$ est donc une des substitutions qui n'altèrent pas Φ, c'est-à-dire une substitution du groupe H :

$$g_\alpha k g_\alpha^{-1} = h.$$

Multiplions à gauche par g_α^{-1} et à droite par g_α ; nous obtenons

$$k = g_\alpha^{-1} h g_\alpha,$$

c'est-à-dire que les substitutions qui n'altèrent pas Φ_α sont de la forme $g_\alpha^{-1} h g_\alpha$.

Inversement, toute substitution de cette forme possède la même propriété. En effet, pour transformer Φg_α par la substitution $g_\alpha^{-1} h g_\alpha$, on peut d'abord transformer cette fonction par g_α^{-1}, ce qui donne $\Phi g_\alpha g_\alpha^{-1} = \Phi$, et transformer ensuite le résultat obtenu Φ par la substitution $h g_\alpha$. Or on a

$$\Phi h g_\alpha = \Phi g_\alpha ;$$

donc la substitution considérée reproduit Φ_α.

Il résulte de là, que :

1° *les substitutions obtenues en faisant sur une substitution quelconque* h, *de* H, *l'opération*

$$g_\alpha^{-1} h g_\alpha$$

forment un groupe H_α ;

2° *ce groupe* H_α *admet la fonction* Φ_α *comme invariant caractéristique.*

Examinons maintenant d'un peu plus près l'opération $g^{-1}hg$; on dit que la substitution que cette opération fait correspondre à la substitution h est la *transformée* de h par g. Soient : (α, β, γ) un cycle de h, α', β', γ' les lettres que la substitution g substitue à α, β, γ ; il est aisé de voir quel est l'effet de l'opération $g^{-1}hg$. La substitution g^{-1} remplace en effet respectivement les lettres α', β', γ' par les lettres α, β, γ, la substitution h remplace ensuite α, β, γ par β, γ, α, et enfin la substitution g remplace β, γ, α par β', γ', α' ; la substitution $g^{-1}hg$ remplace donc α', β', γ' par $\beta' \gamma', \alpha'$, c'est-à-dire comprend le cycle $(\alpha', \beta', \gamma')$. Il résulte de là que les deux

substitutions h et $g^{-1}hg$ sont *semblables*, c'est-à-dire ne diffèrent que par les noms des lettres qui y figurent ; nous venons en effet de montrer qu'à tout cycle de l'une correspond dans l'autre un cycle portant sur le même nombre de lettres.

Les λ groupes $H_1 = H$, $H_2 = g_2^{-1}Hg_2, \ldots$, $H_\lambda = g_\lambda^{-1}Hg_\lambda$ qu'on obtient en transformant les substitutions de H par $g_1 = 1$, $g_2, \ldots, g_\lambda$ sont dits *semblables*. On dit aussi qu'ils sont *conjugués* dans le groupe G.

En général ces sous-groupes conjugués sont distincts. Il peut arriver qu'ils coïncident ; les λ fonctions conjuguées $\Phi_1 = \Phi, \ldots, \Phi_\lambda$ sont alors des invariants caractéristiques du même groupe H. Ce groupe qui se reproduit lorsqu'on le transforme par une substitution quelconque de G est appelé *sous-groupe invariant* de G.

Revenons maintenant à la considération d'un invariant caractéristique Φ du sous-groupe H de G dont l'indice est λ ; les substitutions de G font acquérir à Φ, λ formes distinctes $\Phi_1 = \Phi, \Phi_2, \ldots, \Phi_\lambda$, la fonction $\Phi_\alpha = \Phi g_\alpha$ étant un invariant caractéristique du groupe $H_\alpha = g_\alpha^{-1}Hg_\alpha$. Nous avons d'ailleurs remarqué que les substitutions de G se partagent en λ séries de q substitutions de la forme $g_\alpha h$, et que si l'on multiplie toutes les substitutions de G par l'une d'entre elles on permute seulement entre elles les diverses séries.

Les substitutions de chacune de ces séries $g_\alpha h$ transforment la fonction Φ en une même fonction Φ_α ; il en résulte qu'une substitution du groupe G remplace la suite $\Phi_1, \Phi_2, \ldots, \Phi_\lambda$ par une simple permutation des mêmes éléments.

On peut encore dire qu'à chaque substitution g de G correspond une substitution γ bien déterminée entre les formes de Φ :

$$\gamma = \begin{pmatrix} \Phi_1 & \Phi_2 & \ldots & \Phi_\lambda \\ \Phi g & \Phi g_2 g & \ldots & \Phi g_\lambda g \end{pmatrix}.$$

Enfin il est évident que si les substitutions g et g' conduisent aux substitutions γ et γ' entre les Φ, la substitution gg' conduira à la substitution $\gamma\gamma'$. Si donc on considère le système des substitutions γ, le produit de deux substitutions du système appartient au système, c'est-à-dire que *les substitutions γ forment un groupe* Γ.

Soit maintenant γ une substitution quelconque de Γ ; nous savons qu'il existe une substitution g entre les x qui produit entre les Φ la substitution γ. Lorsqu'on donne la substitution g, γ est dé-

terminé d'une manière unique ; en est-il de même pour g lorsqu'on donne γ ?

Nous pouvons représenter par kg toutes les substitutions du groupe G, g étant la substitution considérée ; imaginons donc que la substitution kg produise sur la suite Φ le même effet que g. On aura, pour chaque valeur de i comprise entre 1 et λ, l'identité

$$\Phi g_i g = \Phi g_i k g.$$

Transformons les deux membres par la substitution $g^{-1}g_i^{-1}$; nous obtiendrons

$$\Phi = \Phi g_i k g_i^{-1},$$

en remplaçant gg^{-1} par 1 ; d'où il résulte que, quel que soit i, la substitution $g_i k g_i^{-1}$ appartient au sous-groupe H.

L'égalité $g_i k g_i^{-1} = h$ donne d'ailleurs

$$k = g_i^{-1} h g_i,$$

c'est-à-dire que k appartient au sous-groupe H_i quel que soit i ; k est donc une substitution du sous-groupe K formé de toutes les substitutions communes à $H_1, H_2, \ldots, H_\lambda$.

Inversement, il est clair que toute substitution k de ce sous-groupe, n'altérant aucune des fonctions $\Phi_1, \Phi_2, \ldots, \Phi_\lambda$, la substitution kg produit toujours sur la suite $\Phi_1, \Phi_2, \ldots, \Phi_\lambda$ le même effet que la substitution g. Supposons alors que le groupe K soit d'ordre r ; l'ordre du groupe Γ des substitutions entre les Φ sera le quotient $\frac{p}{r}$.

Il existe donc entre les groupes G et Γ une correspondance définie de la manière suivante :

1° *A une substitution* g *de* G *correspond une substitution* γ *de* Γ. *A une substitution* γ *de* Γ *correspondent* r *substitutions de* G ;

2° *Au produit* gg' *de deux substitutions de* G *correspond le produit* $\gamma\gamma'$ *des substitutions correspondantes de* Γ.

Lorsque deux groupes G et Γ sont liés de telle sorte, on dit que Γ est *isomorphe* à G. L'isomorphisme est dit *mériédrique* lorsque le nombre r est différent de l'unité ; les deux groupes G et Γ sont alors d'ordre différent.

Si au contraire on a $r = 1$, c'est-à-dire si les deux groupes ont le même ordre, l'isomorphisme est appelé *holoédrique* ; la correspon-

dance entre Γ et G est alors réciproque et l'on peut dire que G est isomorphe à Γ.

Cette définition étant donnée, revenons aux groupes G et Γ qui nous y ont conduit. A la substitution 1 de Γ correspondent évidemment les r substitutions k qui constituent le groupe K formé des substitutions communes à $H_1, H_2, \ldots, H_\lambda$; à une substitution γ quelconque de Γ correspondront de même les r substitutions distinctes

$$gk \qquad \text{ou} \qquad kg,$$

dans lesquelles expressions k représente une substitution quelconque de K et g une des substitutions de G qui correspond à γ.

Considérons un élément quelconque Φ_α de la suite $\Phi_1, \Phi_2, \ldots, \Phi_\lambda$; nous savons qu'il existe une substitution g_α qui, appliquée aux x, remplace Φ_1 par Φ_α, et que toutes les substitutions hg_α ou $g_\alpha . g_\alpha^{-1} h g_\alpha$ produisent sur Φ_1 le même effet; il résulte alors des remarques précédentes qu'il existe précisément $\frac{q}{r}$ substitutions du groupe Γ qui remplacent Φ_1 par Φ_α, chacune d'entre elles correspondant à r substitutions entre les x, de la forme kg. On en conclut d'une manière générale qu'*il existe toujours dans* Γ, $\frac{q}{r}$ *substitutions qui transforment* Φ_β *en* Φ_α, *quels que soient les indices* α *et* β.

Supposons en particulier que H soit un sous-groupe invariant de G, le groupe K coïncidera avec H et on l'aura $r = q$. A une substitution γ de Γ correspondront donc les q substitutions gh; l'ordre du groupe Γ sera $\frac{p}{q}$, c'est-à-dire précisément le nombre λ des fonctions Φ. On sait qu'un groupe de substitutions de λ lettres et d'ordre λ est appelé *groupe normal*.

70. Terminons ces généralités sur les groupes de substitutions en donnant quelques théorèmes dont nous aurons plus loin à faire usage.

Les substitutions communes à deux groupes G_a *et* G_b *forment évidemment un groupe qui est le plus grand sous-groupe commun à* G_a *et* G_b. Ceci s'étend à un nombre quelconque de groupes. Si en particulier on suppose que $H_1, H_2, \ldots, H_\lambda$ aient, en dehors de la substitution identique, des substitutions communes, ces substitutions formeront un groupe K qui sera un sous-groupe invariant de G.

Ce sera donc aussi *a fortiori* un sous-groupe invariant de H ou d'un quelconque des conjugués de H.

Soit H un sous groupe invariant de G; la substitution $g^{-1}hg$ transformée d'une substitution de H par une substitution quelconque de G appartient à H. On peut donc la représenter par hh', h' étant une substitution bien déterminée de H, et de l'égalité

$$g^{-1}hg = hh'$$

on déduit

$$hg = gh.h',$$

ce qu'on énonce en disant : *Les substitutions g et h sont échangeables aux substitutions près du groupe* H.

En particulier si h' est constamment la substitution unité, les substitutions g et h sont simplement échangeables.

On appelle *groupes abéliens* ceux qui sont formés uniquement de substitutions échangeables. Il existe de tels groupes : les groupes formés des puissances d'une substitution en sont évidemment. Si g et h sont deux substitutions d'un groupe abélien, on a toujours $g^{-1}hg = h$, c'est-à-dire que *les sous-groupes d'un groupe abélien sont tous des sous-groupes invariants.*

Les substitutions échangeables avec une substitution quelconque s forment un groupe. Si on a en effet

$$sa = as, \qquad sb = bs\ ,$$

on en déduit $sa.b = a.sb = ab.s$, c'est-à-dire que ab est échangeable avec s. Ce groupe comprend évidemment toutes les substitutions qui sont des puissances de s; les autres substitutions du groupe sont d'ailleurs également échangeables avec les puissances de s. Par exemple

$$s^2a = s.sa = s.as = sa.s = as^2.$$

En représentant par S le groupe formé des puissances de s on peut écrire $S = a^{-1}Sa$, c'est-à-dire que S est un sous-groupe invariant du groupe formé des substitutions échangeables à s.

Plus généralement, les substitutions échangeables *à un groupe* H c'est-à-dire échangeables aux substitutions de H, *aux substitutions près du même groupe* H, forment un groupe G dont H est un sous-groupe invariant. Des relations

$$ha = ah',$$

$$hb = bh'',$$

on déduit en effet $hab = a.h'b = ab.h'''$, ce qui démontre que les substitutions $a, b, \ldots$ forment un groupe G. Le groupe H est d'ailleurs un sous-groupe invariant de G, car pour toute substitution a de G on a

$$a^{-1}ha = h'.$$

J'ajoute que *le groupe* G *est le plus grand parmi ceux qui possèdent* H *comme sous-groupe invariant*. Soit en effet G' le plus grand de ces groupes et g une substitution quelconque de G'; on a

$$g^{-1}hg = h' \qquad \text{ou} \qquad hg = gh.h'',$$

d'où il résulte que g appartient à G.

IV. — Théorèmes de Lagrange.

71. Nous sommes maintenant en mesure d'étudier d'une façon précise la classification en *genres* donnée plus haut pour les fonctions rationnelles de $x_1, x_2, \ldots, x_n$ et de mettre en évidence l'importance de cette classification. On observe immédiatement que toute fonction rationnelle des x à coefficients entiers est le quotient d'une fonction entière, à coefficients entiers, des mêmes lettres, par une fonction entière à coefficients entiers des fonctions symétriques élémentaires $p_1, p_2, \ldots, p_n$; nous pouvons donc nous borner à considérer ici les fonctions entières des x, à coefficients entiers; les résultats obtenus s'étendront d'eux-mêmes aux fonctions rationnelles. Rappelons d'abord quelques-uns des résultats acquis :

Toute fonction entière des x à coefficients entiers est invariant caractéristique d'un certain groupe de substitutions des x.

Tout groupe de substitutions des x possède des invariants caractéristiques entiers en $x_1, x_2, \ldots, x_n$ et à coefficients entiers; nous avons appris à en former.

Si l'on considère un groupe G et l'un de ses sous-groupes H, d'indice λ, tout invariant caractéristique Φ de H prend, par les diverses substitutions de G, λ formes distinctes

$$\Phi_1 = \Phi, \Phi_2, \ldots, \Phi_\lambda,$$

qui sont les fonctions conjuguées de Φ dans le groupe G. Chacune de ces fonctions Φ_α est un invariant caractéristique pour l'un des groupes conjugués de H dans G, groupe que nous avons désigné

par H_α. Enfin, les diverses substitutions des x qui constituent le groupe G font éprouver aux Φ des substitutions formant un groupe isomorphe Γ et ce groupe Γ renferme toujours des substitutions qui remplacent Φ_1 par Φ_α, quel que soit Φ_α.

Nous nous proposons de rechercher les relations qui lient entre eux deux invariants caractéristiques d'un même groupe ou de deux groupes ayant entre eux des rapports simples, tels qu'un groupe et un de ses sous-groupes, deux groupes conjugués, etc. On commencera par étudier les liaisons qui existent entre les invariants caractéristiques du groupe symétrique et ceux d'un groupe quelconque, c'est-à-dire *entre les fonctions symétriques élémentaires* $p_1, p_2, \ldots, p_n$ *et une fonction entière quelconque des* x *à coefficients entiers.*

Soit donc Φ une fonction entière non symétrique des x, elle est pour un certain groupe G un invariant caractéristique ; désignons par λ l'indice de ce groupe dans le groupe symétrique, c'est-à-dire supposons que ce groupe renferme $\frac{n!}{\lambda}$ substitutions distinctes ; à la fonction Φ seront associées $(\lambda - 1)$ fonctions $\Phi_2, \Phi_3, \ldots, \Phi_\lambda$, qui s'en déduisent par toutes les substitutions des x, et les éléments de la suite
$$\Phi_1 = \Phi, \Phi_2, \ldots, \Phi_\lambda$$
sont seulement échangés entre eux par l'une de ces substitutions.

Le produit $(X - \Phi_1)(X - \Phi_2) \ldots (X - \Phi_\lambda)$ demeure alors invariable par toute substitution des x et par suite les coefficients des diverses puissances de X y sont des fonctions entières à coefficients entiers de $p_1, p_2, \ldots, p_n$. On conclut de là que les Φ sont les racines d'une équation de degré λ de la forme

$$X^\lambda - A_1 X^{\lambda-1} + A_2 X^{\lambda-2} - \cdots \pm A_\lambda = 0,$$

où les A sont des fonctions entières des p, à coefficients entiers ; cette équation porte le nom de *résolvante de Lagrange relative à la fonction* Φ.

Nous allons en signaler immédiatement des propriétés importantes :

Il est clair que *si nous regardons les* x *comme des indéterminées*, assujetties uniquement à satisfaire aux conditions nécessaires pour qu'on en puisse définir comme on l'a fait plus haut les fonctions entières à coefficients entiers, toute relation entière à coefficients entiers entre les éléments $\Phi_1, \Phi_2, \ldots, \Phi_\lambda, p_1, p_2, \ldots, p_n$ conduit à une identité en $x_1, x_2, \ldots, x_n$ quand on remplace ces éléments par

leur expression à l'aide des x. Cette identité se transforme donc en une autre identité lorsqu'on effectue sur les x une substitution quelconque, et si l'on remarque que, les p étant des éléments invariables par ces transformations, les Φ subissent les substitutions d'un groupe Σ isomorphe au groupe symétrique S, on pourra en conclure que *toute relation entière à coefficients entiers en* $\Phi_1, \Phi_2, \ldots, \Phi_\lambda, p_1, p_2, \ldots, p_n$ *se transforme en une autre relation également vérifiée par les mêmes éléments, lorsqu'on effectue sur les* Φ *une substitution quelconque du groupe* Σ.

Si l'on considère en particulier les relations qui peuvent exister entre Φ_1 et les fonctions symétriques élémentaires, on voit que chacune d'elles sera également satisfaite par $\Phi_2, \Phi_3, \ldots, \Phi_\lambda$, puisqu'il existe dans le groupe Σ des substitutions qui remplacent Φ_1 par Φ_α, quel que soit α. On conclut de là que *la résolvante de Lagrange relative à la fonction* Φ *est irréductible, lorsque* $p_1, p_2, \ldots, p_n$ *sont des indéterminées*, c'est-à-dire *dans le domaine naturel d'intégrité* $[p_1, p_2, \ldots, p_n]$.

Toutes les relations entières ou rationnelles à coefficients entiers entre Φ_1 et les p sont donc des conséquences nécessaires de la relation

$$\Phi_1^\lambda - A_1\Phi_1^{\lambda-1} + A_2\Phi_1^{\lambda-2} - \cdots \pm A_\lambda = 0.$$

Inversement, considérons une fonction entière à coefficients entiers des éléments $\Phi_1, \Phi_2, \ldots, \Phi_\lambda, p_1, p_2, \ldots, p_n$ et supposons qu'elle demeure invariable par toutes les substitutions du groupe Σ, on pourra en conclure que la fonction des x obtenue en remplaçant ces éléments par leur expression à l'aide des x demeure invariable par toute substitution. Cette fonction s'exprime donc et d'une seule manière, à l'aide de $p_1, p_2, \ldots, p_n$, sous forme entière à coefficients entiers. *Les invariants entiers du groupe* Σ *sont par conséquent des fonctions entières des* p *à coefficients entiers*, et cette proposition rapprochée des précédentes montre que : *La résolvante de Lagrange relative à la fonction* Φ *appartient, dans le domaine* $[p_1, p_2, \ldots, p_n]$, *à la classe particulière définie par le groupe* Σ.

72. Désignons maintenant par H un sous-groupe de G, d'indice μ, c'est-à-dire un groupe d'ordre $\frac{n!}{\lambda\mu}$, par ψ un invariant caractéristique, toujours entier, de H, et proposons-nous de déterminer

les relations qui existent entre ψ et la fonction Φ déjà considérée.

Nous poserons $\rho = \lambda\mu$ et nous désignerons par

$$\psi_1 = \psi, \psi_2, \ldots, \psi_\rho$$

les diverses fonctions conjuguées de ψ dans le groupe symétrique ; soient de même $\Phi_1 = \Phi, \Phi_2, \ldots, \Phi_\rho$ les expressions qui dérivent de Φ en faisant sur les x les mêmes substitutions, expressions parmi lesquelles d'ailleurs λ seulement sont distinctes ; il est clair que la fonction entière

$$\frac{E(y)}{y-\psi_1}\cdot\Phi_1 + \cdots + \frac{E(y)}{y-\psi_\rho}\cdot\Phi_\rho,$$

où l'on a posé

$$E(y) = (y-\psi_1)(y-\psi_2)\ldots(y-\psi_\rho),$$

demeure invariable par toute substitution des x. On a donc identiquement par rapport aux x et à y :

$$\frac{E(y)}{y-\psi_1}\cdot\Phi_1 + \cdots + \frac{E(y)}{y-\psi_\rho}\cdot\Phi_\rho = F(y, p_1, \ldots, p_n),$$

le second membre étant un polynome entier à coefficients entiers.

Comme on a, d'autre part,

$$E(y) = (y-\psi_1)E'(\psi_1) + \frac{1}{1.2}(y-\psi_1)^2E''(\psi_1) + \cdots,$$

on en déduit, en remplaçant y par ψ_1, l'identité en x :

$$E'(\psi_1).\Phi_1 = F(\psi_1, p_1, \ldots, p_n),$$

et si l'on observe que l'expression $E'(\psi_1)$, identique au produit

$$(\psi_1-\psi_2)\ldots(\psi_1-\psi_\rho),$$

n'est pas identiquement nulle en $x_1, x_2, \ldots, x_n$, on en conclura que *tout invariant entier*, Φ_1, *du groupe* G *s'exprime rationnellement à l'aide d'un invariant caractéristique*, ψ_1, *du sous-groupe* H *de* G *et des fonctions symétriques* $p_1, p_2, \ldots, p_n$.

On peut ajouter que le dénominateur de cette expression peut être débarrassé de ψ_1 ; si l'on désigne en effet, par $D(p)$ le discriminant non identiquement nul du polynome $E(y)$, discriminant défini par l'identité

$$M(y, p).E(y) + N(y, p).E'(y) = D(p),$$

on aura

$$\Phi_1 = \frac{F(\psi_1, p).N(\psi_1, p)}{D(p)},$$

et le second membre sera *le quotient d'un polynome entier en* $\psi_1, p_1, \ldots, p_n$ *à coefficients entiers, par le discriminant de* ψ_1.

Deux conséquences de la proposition précédente doivent être signalées tout de suite :

Supposons que le groupe H se réduise au groupe G lui-même ; on pourra dire : *Deux invariants caractéristiques entiers d'un même groupe sont fonction rationnelle l'un de l'autre dans le domaine* $[p_1, p_2, \ldots, p_n]$. Tous les invariants d'un groupe sont donc des fonctions rationnelles d'un invariant caractéristique de ce groupe et des éléments $p_1, p_2, \ldots, p_n$.

Supposons que le groupe H se réduise à la substitution identique. la fonction ψ variera par toute substitution ; on conclut donc de là que *toute fonction entière des* x *à coefficients entiers est aussi fonction rationnelle d'une fonction à* $n!$ *formes, dans le domaine* $[p_1, p_2, \ldots, p_n]$.

Revenons à la relation

$$E'(\psi_1).\Phi_1 - F(\psi_1, p_1, \ldots, p_n) = 0$$

établie plus haut, pour étudier sa nature lorsqu'on l'ordonne par rapport à ψ_1. Pour cela nous observerons avec Lagrange que le produit $(y-\psi_1)(y-\psi_2)\ldots(y-\psi_\mu)$, où $\psi_1, \psi_2, \ldots, \psi_\mu$ désignent les fonctions conjuguées de ψ_1 dans le groupe G, est un invariant du groupe G. On conclut de là et d'une des propositions qu'on vient d'énoncer que ψ_1 vérifie une équation d'ordre μ,

$$\psi^\mu - B_1\psi^{\mu-1} + B_2\psi^{\mu-2} - \cdots \pm B_\mu = 0,$$

dont les coefficients sont des fonctions rationnelles de $p_1, p_2, \ldots, p_n$ et d'un invariant caractéristique de G, par exemple Φ_1.

Si l'on considère une relation entière quelconque à coefficients entiers entre $\psi_1, \ldots, \psi_\mu, \Phi_1$ et les fonctions symétriques $p_1, \ldots, p_n$ comme elle se transforme en identité lorsqu'on y remplace ces éléments par leur expression à l'aide des x, elle restera vraie quand on effectuera sur les x une substitution quelconque. Effectuons en particulier une substitution du groupe G ; les éléments $\Phi_1, p_1, \ldots, p_n$ demeureront inaltérés et les ψ seront transformés par une substitution d'un groupe Γ, isomorphe à G ; on en conclut que *toute relation entière à coefficients entiers entre* $\psi_1, \ldots, \psi_\mu, \Phi_1$ *et les* p *demeure vraie lorsqu'on effectue sur les* ψ *une substitution du groupe* Γ.

En particulier toute relation de cette nature entre ψ_1, Φ_1 et les p,

sera également vérifiée par $\psi_2, \ldots, \psi_\mu$, d'où il résulte que *l'équation*

$$Y^\mu - B_1 Y^{\mu-1} + B_2 Y^{\mu-2} - \cdots \pm B_\mu = 0$$

est irréductible dans le domaine $[\Phi_1, p_1, p_2, \ldots, p_n]$, domaine formé par l'adjonction au domaine naturel $[p_1, \ldots, p_n]$ d'une fonction algébrique, Φ_1, des p, définie par la relation irréductible

$$\Phi_1^\lambda - A_1 \Phi_1^{\lambda-1} + \cdots \pm A_\lambda = 0.$$

Réciproquement, toute fonction entière à coefficients entiers de $\psi_1, \ldots, \psi_\mu, \Phi_1$ et $p_1, \ldots, p_n$, qui demeure inaltérée par les substitutions du groupe Γ, est également une fonction entière des x qui demeure inaltérée par toute substitution du groupe G, c'est-à-dire peut s'exprimer sous forme rationnelle à l'aide de Φ_1 et des p. On peut donc dire que *l'équation*

$$Y^\mu - B_1 Y^{\mu-1} + \cdots \pm B_\mu = 0$$

appartient dans le domaine $[\Phi_1, p_1, \ldots, p_n]$ *à la classe particulière définie par le groupe* Γ.

Nous savons d'autre part que ψ_1 vérifie dans le domaine naturel $[p_1, \ldots, p_n]$ une équation irréductible de degré $\lambda\mu$, qui appartient dans ce domaine à la classe définie par un groupe Σ_H isomorphe au groupe symétrique S; il serait facile de montrer les rapports qui existent entre les groupes Σ_G, Γ et Σ_H, en désignant par Σ_G le groupe représenté jusqu'ici par Σ; nous nous bornerons à faire à ce sujet la remarque suivante :

Si l'on représente par $\psi_{i,j}$ $(j = 1, 2, \ldots, \mu)$ les diverses formes de ψ qui vérifient l'identité

$$Y^\mu - B_1^{(i)} Y^{\mu-1} + \cdots \pm B_\mu^{(i)} = 0,$$

où les B^i sont des fonctions rationnelles de Φ_i, toute substitution des x qui laisse invariable Φ_i échange entre elles ces diverses formes et toute substitution qui remplace Φ_i par Φ_k, remplace aussi l'ensemble des éléments $\psi_{i,j}$ $(j = 1, 2, \ldots, \mu)$ par l'ensemble des éléments $\psi_{k,j}$ $(j = 1, 2, \ldots, \mu)$.

73. Les résultats que nous venons d'acquérir ont été obtenus en supposant que les x ou les p sont des indéterminées ; ils expriment, si l'on veut, des propriétés qui sont vraies *pour l'ensemble* des équations qu'on obtient en fixant les p ; mais ils ne sont pas applicables, du moins sans préparation, dans le cas où les p sont

déterminés. Il importe donc de chercher comment ils doivent être modifiés et c'est ce qu'il est facile de trouver.

Nous considérerons d'abord le théorème relatif à l'expression explicite d'une fonction Φ_1 des x à l'aide d'une autre fonction ψ_1 et des p; il est aisé de voir que ce théorème devient illusoire lorsque l'on a $E'(\psi_1) = 0$, c'est-à-dire quand le discriminant $D(p)$ est nul. Nous allons montrer qu'il est toujours possible de choisir la fonction entière ψ_1 de telle sorte que ce fait ne se présente pas, c'est-à-dire qu'*il existe dans tout genre, sous la condition unique que les x soient distincts, des fonctions à discriminant non nul.*

Observons, dans ce but, que le discriminant de ψ_1, c'est-à-dire le produit $\prod (\psi_{i,j} - \psi_{i',j'})$ $(i, i' = 1, 2, \ldots, \lambda)$ $(j, j' = 1, 2, \ldots, \mu)$, où l'on exclut les cas $i = i'$, $j = j'$, peut s'écrire à un facteur près sous forme de déterminant de la manière suivante :

$$\begin{vmatrix} \psi_{1,1} & (\psi_{1,1})^2 & \ldots & (\psi_{1,1})^{\lambda\mu} \\ \psi_{1,2} & (\psi_{1,2})^2 & \ldots & (\psi_{1,2})^{\lambda\mu} \\ \ldots & \ldots & \ldots & \ldots \\ \psi_{1,\mu} & (\psi_{1,\mu})^2 & \ldots & (\psi_{1,\mu})^{\lambda\mu} \\ \psi_{2,1} & (\psi_{2,1})^2 & \ldots & (\psi_{2,1})^{\lambda\mu} \\ \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots \\ \psi_{\lambda,\mu} & (\psi_{\lambda,\mu})^2 & \ldots & (\psi_{\lambda,\mu})^{\lambda\mu} \end{vmatrix}$$

Ajoutons aux éléments de la ligne de rang μ les éléments correspondants des $(\mu - 1)$ lignes précédentes ; procédons de même pour toutes les lignes dont le rang est multiple de μ, de telle sorte que la ligne de rang $i\mu$ devienne

$$\sum_{k=1}^{k=\mu} \psi_{i,k} \qquad \sum_{k=1}^{k=\mu} (\psi_{i,k})^2, \qquad \ldots, \qquad \sum_{k=1}^{k=\mu} (\psi_{i,k})^{\lambda\mu}.$$

On voit que les éléments de la ligne de rang $i\mu$ sont des invariants pour l'un des groupes conjugués de G dans le groupe symétrique ; si l'on considère, par conséquent, l'expression

$$\chi_1 = m_1 \sum_{k=1}^{k=\mu} \psi_{1,k} + m_2 \sum_{k=1}^{k=\mu} (\psi_{1,k})^2 + \cdots + m_{\lambda\mu} \sum_{k=1}^{k=\mu} (\psi_{1,k})^{\lambda\mu},$$

où les m désignent des entiers indéterminés, χ_1 est un invariant du groupe G. Admettons maintenant qu'ayant fixé les déterminations des p, on ait pu choisir l'invariant caractéristique ψ_1 du groupe H de telle sorte que son discriminant ne soit pas nul ; il existe alors des entiers m pour lesquels les expressions $\chi_1, \ldots, \chi_\lambda$ prennent des déterminations distinctes sans quoi le déterminant écrit plus haut aurait des lignes identiques c'est-à-dire serait nul, ce qui est contraire à l'hypothèse qu'on vient de faire. On en conclut qu'on peut former un invariant caractéristique χ_1, d'un groupe G qui renferme H, dont toutes les déterminations sont distinctes.

Mais tout groupe renferme la substitution identique et nous avons établi dans le chapitre précédent, que si le discriminant des x est différent de zéro on sait former des fonctions à $n!$ formes dont toutes les déterminations sont distinctes ; nous savons donc former pour tout genre des fonctions à discriminant non nul.

On déduit de là qu'il est toujours possible d'appliquer le théorème qui donne Φ_1 en fonction de ψ_1 et des p, en choisissant convenablement l'invariant caractéristique ψ_1.

Passons maintenant aux théorèmes relatifs aux divers rapports qu'ont entre elles des fonctions entières des x, à coefficients entiers ; on voit clairement que tous ces théorèmes sont des conséquences immédiates du fait que toutes les relations que l'on peut former sont des identités en $x_1, x_2, \ldots, x_n$, c'est-à-dire demeurent vraies quand on les transforme par les substitutions du groupe symétrique S. Nous savons qu'il n'en est plus toujours de même quand les p sont déterminés et que les seules substitutions qui transforment des relations vraies en relations également vraies sont les substitutions d'un certain groupe G, appelé *groupe de l'équation*

$$x^n - p_1 x^{n-1} + \cdots \pm p_n = 0.$$

Les théorèmes applicables ici sont donc ceux que l'on a obtenus en introduisant explicitement dans le calcul, avec les fonctions symétriques élémentaires $p_1, p_2, \ldots p_n$, un invariant caractéristique, Φ_1, du groupe G. C'est ce qui sera exprimé d'une manière plus nette encore dans le chapitre suivant.

CHAPITRE VI

LES GROUPES RÉSOLUBLES

I. — La résolution algébrique des équations.

74. Étant donnée une équation algébrique entière irréductible

$$f(x) = 0,$$

nous avons vu qu'elle définit n symboles et nous avons appris dans quelle mesure il était possible de distinguer ces symboles entre eux. Nous savons que, les notations étant fixées, les diverses substitutions permises entre les lettres $x_1, x_2, \ldots, x_n$ sont précisément les substitutions d'un certain groupe, le groupe de l'équation; toutes les relations rationnelles entre les racines restent vérifiées lorsqu'on effectue sur elles une de ces substitutions, et toute autre substitution les transforme en nouvelles relations incompatibles avec les anciennes.

Les résultats obtenus dans le chapitre précédent relativement aux liaisons qui existent entre les diverses fonctions rationnelles de n éléments distincts, vont nous permettre de préciser les diverses méthodes que l'on peut employer pour *parvenir à une expression explicite des x en introduisant, dans le calcul, d'autres nombres algébriques bien définis*, c'est-à-dire de traiter la question de la *résolution algébrique* des équations.

Nous commencerons par examiner le cas où les nombres algébriques, que l'on introduit dans le calcul, s'expriment rationnellement à l'aide des x, c'est-à-dire où l'on ne fait appel qu'à des éléments pris dans le domaine de rationalité $(x_1, x_2, \ldots, x_n)$.

Désignons par G le groupe de l'équation $f(x) = 0$, nous savons que si une fonction rationnelle φ de $x_1, x_2, \ldots, x_n$ est un invariant caractéristique d'un sous-groupe de G d'indice λ, elle prend par les substitutions de G, λ formes distinctes $\varphi_1, \varphi_2, \ldots, \varphi_\lambda$. Nous savons de plus que si les sous-groupes conjugués du sous-groupe donné ont en commun un sous-groupe (invariant dans G) d'ordre k, les substitutions opérées sur la suite

$$\varphi_1, \varphi_2, \ldots, \varphi_\lambda$$

lorsqu'on lui applique les diverses substitutions de G, forment un groupe Γ isomorphe à G, mais renfermant k fois moins de substitutions. Si k est égal à l'unité, c'est-à-dire si les divers groupes conjugués n'ont en commun que la substitution identique, l'isomorphisme est holoédrique, de sorte que l'indétermination des φ est exactement de même nature que l'indétermination des x; de plus lorsqu'on fixe le sens des φ, le sens des x se trouve fixé. Au contraire lorsque le nombre k est supérieur à 1, l'indétermination des φ est de nature plus simple que l'indétermination des x, mais, d'autre part, lorsqu'on fixe le sens des φ, les x ne se trouvent pas absolument déterminés, vu que l'on peut encore effectuer sur eux les substitutions d'un groupe d'ordre k.

D'une manière plus précise, si la fonction φ est choisie de telle sorte que ses diverses formes prennent des déterminations distinctes, l'ensemble des relations rationnelles entre les φ demeure invariable par toutes les substitutions d'un groupe Γ isomorphe à G, isomorphe holoédriquement lorsque k est égal à 1, mériédriquement dans le cas contraire. On peut encore dire que les φ sont les racines d'une équation irréductible à coefficients entiers dont le groupe est précisément Γ.

Si l'on considère l'ensemble des relations rationnelles entre les φ et les x, cet ensemble varie par toute substitution des x ou des φ, et conduit à des relations incompatibles avec les premières lorsque k est l'unité ; il demeure invariable par les substitutions des x qui appartiennent à un groupe K d'ordre k, lorsque k est différent de l'unité, mais il varie toujours par toute substitution des φ. Dans le premier cas les x peuvent s'exprimer rationnellement à l'aide des φ; dans le second ils sont racines d'une équation irréductible dans le domaine $(\varphi_1, \varphi_2, \ldots, \varphi_\lambda)$ et qui appartient dans ce domaine à la classe définie par le groupe K.

75. Examinons maintenant le cas général où l'on introduit dans le calcul des nombres algébriques quelconques, définis par une équation irréductible $h(y) = 0$, n'ayant *a priori* aucune relation avec l'équation donnée $g(x) = 0$.

Nous avons vu qu'étant données deux équations irréductibles

$$g(x) = 0,$$
$$h(y) = 0,$$

de degrés m et n, dont nous désignons les racines par $x_1, x_2, \ldots, x_m$; $y_1, y_2, \ldots, y_n$, il correspond à chacune de ces équations un groupe, le premier de degré m, le second de degré n; nous savons obtenir ces groupes, à l'aide de la résolvante de Galois de chaque équation. Si nous considérons à la fois les symboles x et les symboles y, il est clair que, pour savoir quelle est l'indétermination de l'ensemble de ces symboles, il nous suffit de former la résolvante générale du système

$$S_1 = a_1, \quad \ldots, \quad S_m = a_m,$$
$$T_1 = b_1, \quad \ldots, \quad T_p = b_p,$$

et d'étudier cette résolvante; on retombe ainsi sur un problème posé dans le chapitre IV et dont nous allons maintenant approfondir la solution. Nous observerons immédiatement que la résolvante considérée est aussi celle du système

$$U_1 = c_1, \quad \ldots, \quad U_{m+p} = c_{m+p},$$

qu'on obtient en écrivant les relations entre les coefficients et les racines de l'équation *réductible* $g(z)h(z) = 0$. Si nous désignons par Γ le groupe des substitutions des x et des y qui n'altèrent point l'ensemble des relations rationnelles entre ces symboles, il sera par conséquent légitime d'étendre la définition donnée plus haut du groupe d'une équation et de dire que Γ *est le groupe de l'équation réductible* $g(z).h(z) = 0$.

D'ailleurs il est bien évident que toutes les substitutions du groupe Γ de degré $m + p$ que l'on obtient ainsi, devant laisser invariantes toutes les relations rationnelles entre $x_1, x_2, \ldots, x_m$, $y_1, y_2, \ldots, y_p$, devront se borner à échanger les x entre eux et les y entre eux, car ces relations rationnelles conduisent aux identités en x et y :

$$g(x) = (x - x_1)(x - x_2) \ldots (x - x_n),$$

$$h(y) = (y - y_1)(y - y_2) \ldots (y - y_n).$$

Le groupe Γ est dit *intransitif* car il ne renferme par exemple aucune substitution qui remplace x_1 par y_1; on appelle au contraire groupe *transitif* un groupe dans lequel se trouve au moins une substitution remplaçant une lettre donnée, mais quelconque, par une lettre quelconque. Nous venons de voir que le groupe d'une équation réductible est intransitif; réciproquement, *si le groupe d'une équation est intransitif, l'équation est réductible*; il est en effet aisé de voir que dans ce cas les racines de l'équation se partagent en plusieurs séries telles que les substitutions du groupe échangent entre elles les racines d'une même série; dès lors il est clair que les fonctions symétriques des racines de l'une quelconque de ces séries sont invariables par les substitutions du groupe et par suite rationnelles; donc l'équation est réductible. De ces deux propositions, il résulte que la définition donnée plus haut du groupe d'une équation réductible, ne peut donner lieu à aucune contradiction.

Revenons au groupe Γ de l'équation

$$g(z)h(z) = 0,$$

et soient G et H les groupes des deux équations

$$g(x) = 0, \qquad h(y) = 0;$$

nous désignerons d'une manière générale par les lettres γ, g, h, affectées d'indices, des substitutions appartenant aux groupes Γ, G, H.

Je dis d'abord que toute substitution γ est de la forme gh, c'est-à-dire que toute substitution de Γ revient à une certaine substitution de G, accompagnée d'une certaine substitution de H. En effet, nous savons déjà que la substitution γ échange d'une part les x entre eux, et d'autre part les y entre eux; on peut donc poser $\gamma = \xi\eta$, la substitution ξ déplaçant seulement les x et la substitution η seulement les y. Nous savons que la substitution γ possède la propriété de laisser invariante toute fonction des x et des y qui est égale à un nombre rationnel; si nous considérons en particulier une fonction φ des x seuls qui possède cette propriété, on a

$$\varphi\gamma = \varphi;$$

mais la substitution η ne déplaçant que les y et φ ne dépendant que des x, on a aussi

$$\varphi\gamma = \varphi\xi\eta = \varphi\xi;$$

donc $\varphi\xi = \varphi$, et par suite la substitution ξ appartient au groupe G de l'équation qui admet les x pour racines ; on verrait de même que η appartient au groupe H ; on a donc $\gamma = gh$. Soit $\gamma' = g'h'$ une autre substitution de Γ ; on a $\gamma\gamma' = ghg'h' = gg'.hh'$, car les substitutions g' et h déplaçant des lettres différentes sont échangeables. Nous pouvons dire que cette relation établit entre les groupes G et H un isomorphisme *doublement mériédrique* ; voici ce que nous devons entendre par là : faisons correspondre à une substitution g de G toutes les substitutions h telles que gh soit une substitution de Γ et de même à une substitution h de H toutes les substitutions g telles que gh appartienne à Γ ; il est clair d'après ce qui précède, que si g et h se correspondent ainsi et aussi g' et h', gg' correspond à hh'.

Il est d'ailleurs possible d'établir une telle correspondance entre deux groupes quelconques ; il suffit en effet de faire correspondre à chaque substitution de l'un d'eux *toutes les substitutions* de l'autre. Si ce cas se présente ici, les substitutions de Γ sont *toutes* les substitutions de la forme gh ; donc si l'on suppose que les y soient *fixés*, c'est-à-dire si l'on considère les substitutions de Γ qui ne déplacent pas les y, elles sont de la forme $g.1$, g étant une substitution quelconque de G : l'indétermination des x est donc la même que si l'on considérait à part l'équation $g(x) = 0$. Dans ce cas, l'introduction dans le calcul des symboles x et des symboles y peut se faire d'une façon complètement indépendante. On remarquera que l'ordre du groupe Γ est égal au produit des groupes G et H ; nous verrons tout à l'heure que cette circonstance *caractérise* le cas que nous venons d'étudier.

76. Supposons maintenant que la correspondance dont il a été question entre les groupes G et H soit telle, qu'à la substitution identique de h correspondent seulement un certain nombre de substitutions de G ; il est d'abord clair que ces substitutions forment un groupe, car le produit de deux d'entre elles correspond au produit de la substitution identique par elle-même. Je dis que de plus ce groupe est un sous-groupe invariant de G ; on peut dire que

cela résulte immédiatement de ce que la substitution identique est un sous-groupe invariant de H ; on peut aussi le démontrer ainsi : soit $g.1$ une substitution de Γ, g' une substitution quelconque de G. Je dis d'abord qu'il existe dans Γ une substitution au moins de la forme $g'h$; il est clair en effet que si dans les substitutions de Γ on supprime tout ce qui est relatif aux y, on doit retrouver le groupe G. Or on a

$$(g'h).(g.1)(g'h)^{-1} = g'gg'^{-1}.1 ;$$

donc $g'gg'^{-1}$ appartient au sous-groupe considéré ; ce sous-groupe K est donc invariant dans G. Désignons par λ son indice et par p et q les ordres des groupes G et H, le groupe K est d'ordre $r = \frac{p}{\lambda}$; je dis qu'il y a dans le groupe Γ précisément r substitutions de la forme gh, h désignant une substitution déterminée de H. En effet, soit $g'h$ celle des substitutions de cette forme dont nous avons démontré l'existence et gh une autre quelconque de la même forme ; la substitution

$$(gh)(g'h)^{-1}$$

appartient à Γ ; elle est de la forme $gg'^{-1}.1$; donc $g'g^{-1}$ appartient au groupe K et l'on a $g = \varkappa g'$, $\varkappa$ désignant une certaine substitution de K. Il est clair d'ailleurs que $\varkappa$ étant une substitution quelconque de K et la substitution $g'h$ appartenant au groupe Γ, il en est de même de la substitution

$$(\varkappa.1)(g'h) = \varkappa.g'.h.$$

On obtient donc toutes les substitutions de la forme gh en multipliant l'une d'entre elles successivement par les r substitutions de K et on obtient ainsi r substitutions distinctes. L'ordre du groupe Γ est donc $r.q = \frac{pq}{\lambda}$.

Nous arrivons ainsi à cette conclusion que si dans le groupe Γ la substitution identique du groupe H se trouve associée avec les substitutions du groupe G formant un sous-groupe invariant K d'indice λ, l'ordre de Γ est d'indice $\frac{pq}{\lambda}$. Il est clair que la réciproque de cette proposition est vraie, c'est-à-dire que si l'ordre de Γ est $\frac{pq}{\lambda}$, il correspond à la substitution identique de H un sous-groupe invariant d'indice λ dans G ; de plus il correspond de

même à la substitution identique de G un sous-groupe invariant d'indice λ dans H.

77. Nous sommes maintenant en mesure de préciser l'influence produite sur le calcul des symboles x par l'introduction des symboles y, ou mieux, en quoi le calcul simultané des symboles x et y diffère du calcul séparé de chacune de ces séries de symboles.

Pour *connaître* le calcul des symboles x, il nous est nécessaire de former une table de structure du groupe (infini et commutatif) que constituent ces symboles et leurs fonctions entières, vis-à-vis des deux modes de composition connus : addition et multiplication. Nous savons que si nous fixons les notations d'une manière arbitraire, mais précise, il subsistera encore dans cette table une certaine symétrie, *précisément indiquée par le groupe* G *de l'équation*, c'est-à-dire que les substitutions de ce groupe pourront être effectuées sans rien altérer. Il en est de même pour ce qui concerne les y et le groupe H. Mais si l'on considère simultanément les x et les y, il ne sera pas permis d'effectuer séparément sur les x les opérations du groupe G et sur les y les opérations du groupe H : les seules substitutions permises sont en effet, par définition, les substitutions du groupe Γ. Si d'ailleurs nous convenons de *fixer* les symboles y, c'est-à-dire de renoncer à les permuter entre eux, les seules substitutions permises seront les substitutions du groupe Γ qui n'altèrent pas les y, c'est-à-dire les substitutions du groupe K. Nous exprimerons ce fait en disant que par l'*adjonction* des y le groupe G de l'équation $g(x) = 0$ est réduit à son sous-groupe invariant K. L'étude du groupe Γ, laquelle comprend celle du groupe G comme cas particulier, se ramène d'après ce qui précède à l'étude successive des groupes H et K ; c'est-à-dire que lorsqu'on a étudié l'équation $h(y) = 0$, l'étude de l'équation $g(x) = 0$ ne dépend plus que du groupe K, et non plus du groupe G. A un autre point de vue, on peut dire que le fait de *considérer comme connues* les racines de l'équation irréductible $h(y)$ réduit le groupe de $g(x)$ à un de ses sous-groupes (*invariant*) d'indice λ ; il est d'ailleurs clair, à cause de la symétrie de tout ce qui précède, que, réciproquement, l'*adjonction* des racines de $g(x)$ réduirait le groupe de $h(y)$ à un de ses sous-groupes invariants d'indice λ.

On a vu d'ailleurs, qu'étant donné un sous-groupe invariant K

d'indice λ du groupe G d'une équation donnée, il est toujours possible de ramener l'étude du groupe de l'équation à l'étude de ce sous-groupe et d'un autre groupe d'ordre λ ; si nous désignons en effet par φ un invariant caractéristique de ce sous-groupe, cet invariant caractéristique prend par les substitutions de G, λ formes distinctes $\varphi_1, \varphi_2, \ldots, \varphi_\lambda$ et si l'on applique à ces λ fonctions toutes les substitutions de G on obtient seulement λ permutations différentes, c'est-à-dire qu'il correspond à ces fonctions un groupe d'ordre λ. Si d'ailleurs on *fixe* l'une de ces permutations, les seules substitutions permises sur les lettres $x_1, x_2, \ldots, x_n$ sont les substitutions du groupe K. On a ainsi ramené l'étude du groupe G à l'étude du groupe K et d'un groupe d'ordre λ.

Ainsi *toute réduction du groupe obtenue par l'adjonction des racines d'une équation irréductible quelconque peut être obtenue aussi par l'adjonction d'une certaine fonction rationnelle des racines de l'équation donnée.*

D'ailleurs une telle réduction n'est possible que si le groupe G admet un sous-groupe invariant ; nous avons vu en effet que si des fonctions conjuguées sont des invariants caractéristiques de groupes n'ayant en commun que la substitution identique, le groupe des substitutions possibles sur les indices de ces fonctions est holoédriquement isomorphe au groupe G.

Ainsi de quelque manière que l'on opère, que l'on cherche à introduire dans le calcul des nombres algébriques quelconques (*), ou bien seulement des fonctions rationnelles des racines, on ne peut espérer une réduction ou pour mieux dire, une décomposition de l'étude du groupe d'une équation donnée, que si ce groupe admet un sous-groupe invariant. D'ailleurs si un groupe admet un sous-groupe invariant, nous avons déjà vu que son étude se ramène à l'étude de deux groupes plus simples, dont l'ordre a pour produit l'ordre du groupe donné.

Nous approfondirons dans le chapitre suivant certaines des questions algébriques qui se rattachent à cette décomposition du groupe ; nous allons l'étudier ici en nous plaçant uniquement au point de vue

(*) Il est clair que, du moment qu'il s'agit ici de résoudre une équation, c'est-à-dire de distinguer le plus possible entre les symboles qu'elle définit, il ne peut être question d'introduire une racine d'une équation irréductible sans les introduire toutes comme nous pouvions le faire dans l'étude d'un domaine algébrique.

de la théorie des substitutions ; d'ailleurs, au point de vue purement abstrait, nous aurons ainsi complètement traité le problème de la résolution des équations, c'est-à-dire de l'étude des symboles qu'elles définissent. Nous aurons en effet *analysé* autant qu'il est possible de le faire la nature de l'indétermination qui subsiste dans la définition de ces symboles, indétermination représentée par le groupe.

II. — Décomposition d'un groupe.

78. Soit G un groupe *composé*, c'est-à-dire un groupe admettant au moins un sous-groupe invariant (un groupe non composé est dit *simple*) et soit H un sous-groupe invariant de G. Supposons qu'il n'existe aucun sous-groupe invariant de G renfermant toutes les substitutions de H et différent de H ; nous dirons que H est un sous-groupe invariant *maximum* de G ; on remarque que cela ne veut pas dire que G n'a pas de sous-groupe invariant d'ordre supérieur à H, mais simplement qu'il n'a pas de sous-groupe invariant d'ordre supérieur à H et comprenant H.

Il est clair d'ailleurs que si H n'est pas un sous-groupe invariant maximum de G, il existe un sous-groupe invariant de G comprenant H et admettant H comme sous-groupe invariant maximum; il est donc possible de former une suite de groupes

$$G,\ G_1,\ G_2,\ \ldots,\ G_k,\ H,$$

tels que chacun d'eux soit sous-groupe invariant maximum du précédent.

Lorsqu'on a une suite de groupes

$$G,\ G_1,\ G_2,\ \ldots,\ G_n,\ 1,$$

commençant par un groupe G, se terminant à la substitution identique et telle que chaque groupe soit un sous-groupe invariant maximum du précédent, on dit que cette suite est une *suite de composition de* G. Tout groupe composé a une ou plusieurs suites de composition, et il résulte de ce qui précède que H étant un sous-groupe invariant quelconque de G, il y a une suite de composition de G qui comprend le groupe H.

Soit

$$(1) \qquad G,\ H,\ I,\ J,\ \ldots,\ M,\ 1$$

une suite de composition de G; désignons par λ l'indice de H dans G, par μ l'indice de I dans H, ..., par ρ l'indice de la substitution identique dans M (c'est-à-dire l'ordre de M); les nombres $\lambda, \mu, \ldots, \rho$ sont dits les *facteurs de composition* de G, relatifs à la suite (1). Nous pouvons énoncer à leur égard la proposition suivante : *Lorsqu'on passe d'une des suites de composition d'un groupe* G *à une autre, les facteurs de composition sont simplement permutés.*

La démonstration de cette proposition va nous fournir l'occasion d'utiliser la notion générale des *groupes d'opérations*, tout en approfondissant la constitution intime des groupes de substitutions.

Soient H un sous-groupe invariant quelconque de G,

$$h_1 = 1, \qquad h_2, \qquad \ldots, \qquad h_p$$

ses substitutions distinctes, λ son indice. Nous avons démontré que toutes les substitutions de G pouvaient être rangées dans le tableau suivant :

$$\begin{array}{cccc} h_1 = 1 & h_2 & \ldots & h_p \\ g_2 & g_2h_2 & \ldots & g_2h_p \\ \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots \\ g_\lambda & g_\lambda h_2 & \ldots & g_\lambda h_p ; \end{array}$$

$g_1 = 1, \; g_2, \ldots, g_\lambda$ sont des substitutions choisies d'une manière connue.

Soient $g_\alpha h_a$ et $g_\beta h_b$ deux des substitutions de G; le produit de ces deux substitutions qui est encore une substitution de G peut s'écrire

$$g_\alpha h_a . g_\beta h_b = g_\alpha . g_\beta h_a . h_b.$$

En effet, le groupe H étant invariant dans G, on a $g_\beta^{-1} h_a g_\beta = h_{a'}$; donc, en multipliant à gauche par g_β,

$$h_a g_\beta = g_\beta h_{a'}.$$

Considérons maintenant le produit $g_\alpha g_\beta$: c'est une substitution $g_\delta h_a$, δ ne dépendant que de α et β. On a donc

$$g_\alpha h_a . g_\beta h_b = g_\delta . h_a h_{a'} h_b$$

ou encore

$$g_\alpha h_a . g_\beta h_b = g_\delta h_e .$$

On a ainsi défini une *composition des lignes de* G, puisqu'une substitution quelconque de la ligne g_α composée avec une substitution

quelconque de la ligne g_β donne toujours une substitution de la ligne g_δ.

Soit op. α l'une quelconque des substitutions de la ligne $g_\alpha h$, la multiplication des opérations ainsi définies est associative, c'est-à-dire que pour obtenir

$$\text{op.}\,\alpha \times \text{op.}\,\beta \times \text{op.}\,\gamma$$

il suffit d'effectuer op. $\alpha \times$ op. β, ce qui donne op. δ, puis la nouvelle multiplication

$$\text{op.}\,\delta \times \text{op.}\,\gamma.$$

Enfin, parmi les opérations considérées il y en a une qui n'a aucun effet, c'est l'opération qui correspond à la ligne

$$h_1 = 1, \qquad h_2, \qquad \ldots, \qquad h_p.$$

Ce sera l'opération identique du système.

Nous avons donc défini un système d'opérations, jouissant des propriétés suivantes :

1° Par un moyen de composition quelconque (multiplication) on passe d'une manière uniforme de deux opérations du système à une autre opération du système ;

2° La multiplication des opérations est associative ;

3° Une même opération composée avec des opérations différentes donne des opérations différentes.

Nous savons que dans ce cas on dit que ces opérations forment un *groupe* (§ 5) et que les propriétés principales des groupes de substitutions s'étendent à de tels systèmes.

Nous désignerons ce groupe par G|H et nous l'appellerons *quotient* de G par H.

79. Deux substitutions de G seront dites *équivalentes* lorsqu'on passe de l'une à l'autre en la multipliant par une substitution de H. Grâce au fait que H est un sous-groupe invariant, on a

$$g_\alpha h_b = h_{b'} g_\alpha,$$

c'est-à-dire qu'on n'a pas besoin de spécifier dans la définition si on multiplie à droite ou à gauche. Il en résulte d'abord que l'équivalence est réciproque, et ensuite que le produit de deux substitutions équivalentes est encore une substitution équivalente à ces deux-là. Les substitutions de G sont ainsi partagées en *classes de substitutions équivalentes*.

Aux substitutions $gh_1, gh_2, \ldots, gh_p$ de G correspond une même opération du groupe d'opérations G|H ; ce nouveau groupe est donc *isomorphe mériédriquement au premier*.

Si le groupe G|H ne renferme pas dans ses opérations toutes les classes de G, les substitutions des classes qu'il contient forment un sous-groupe invariant H' de G. Ce sous-groupe contient le groupe H, car les substitutions de H donnent l'opération identique qui appartient à G|H.

Si H est un sous-groupe invariant maximum de G il n'y a pas de groupe tel que H' ; le groupe d'opérations G|H ne peut avoir de sous-groupe invariant, sans quoi on en déduirait un groupe H' ; donc il est simple.

Enfin ajoutons que l'ordre de G est le produit des ordres de H et de G|H et que le groupe G|H est précisément isomorphe au groupe d'ordre λ dont il a été question plus haut.

Si maintenant nous considérons un groupe G et une suite de composition de ce groupe

$$G, H, I, J, K, \ldots, M, 1,$$

à cette suite correspond un ensemble de groupes d'opérations

$$G \mid H, \qquad H \mid I, \qquad \ldots,$$

qui sont tous *simples*. On appelle ces groupes, *groupes facteurs* du groupe G ; leurs ordres sont précisément les entiers que nous avons appelés précédemment facteurs de composition de G.

80. *La suite des groupes facteurs est seulement permutée lorsqu'on passe d'une des suites de composition de G à une autre.*

Supposons en effet que G possède deux sous-groupes invariants maxima H et H'.

Les substitutions communes à H et H' forment un groupe Γ, et comme la transformée d'une substitution de Γ par une substitution quelconque de G appartient à la fois à H et à H', Γ est un sous-groupe invariant de G, H et H'.

Soient maintenant a et b des substitutions quelconques de H et de H'

$$H = [a, a', a'', \ldots],$$

$$H' = [b, b', b'', \ldots],$$

et c une substitution quelconque de G. Si on combine les substi-

tutions a, a', ... avec les substitutions b, b', ... de toutes les manières possibles, on obtient un groupe qui est contenu dans G et qui contient H et H'. D'ailleurs la transformée d'une substitution $a.b.a'.b'$ par la substitution c peut s'écrire

$$c^{-1}ac.c^{-1}bc.c^{-1}a'c.c^{-1}b'c,$$

forme sous laquelle on reconnaît qu'elle appartient encore au groupe précédent. Ce groupe est donc un sous-groupe invariant de G qui doit renfermer H et H' ; ce ne peut être que le groupe G lui-même.

Le groupe G se partage d'ailleurs en classes de substitutions équivalentes qui dérivent l'une de l'autre par une substitution de Γ. Si nous considérons ensuite les groupes H et H' qui contiennent Γ, ils contiendront entièrement chaque classe de substitutions dont ils contiennent une partie ; donc H et H' sont aussi partagés en classes de la même manière.

Les opérations qui composent entre elles ces classes forment donc des groupes $G|\Gamma$, $H|\Gamma$, $H'|\Gamma$; nous les appellerons G_0, H_0, H'_0.

On sait qu'ils sont respectivement isomorphes à G, H, H' ; on peut en déduire que G_0 est engendré par H_0 et H'_0 qui sont deux de ses sous-groupes invariants maxima. D'ailleurs comme H et H' ont en commun Γ, H_0 et H'_0 auront en commun la seule opération identique.

Soient S, S_1, S_2, ... les opérations de H_0, T, T_1, T_2, ... celles de H'_0. Le produit $T^{-1}S^{-1}TS$ peut s'écrire d'une part $(T^{-1}S^{-1}T)S$, et d'autre part $T^{-1}(S^{-1}TS)$, en vertu de la propriété associative de la multiplication. Il appartient donc à la fois à H_0 et à H'_0 et par conséquent c'est l'opération identique de G_0, d'où $TS = ST$: *Les opérations* S *et* T *sont échangeables.*

Toutes les opérations de G_0 peuvent alors se mettre d'une manière et d'une seule sous la forme $S_\alpha T_\beta$.

En effet, une relation de la forme

$$S_\alpha T_\beta = S_{\alpha'} T_{\beta'}$$

donne

$$S_{\alpha'}^{-1} S_\alpha = T_{\beta'} T_\beta^{-1},$$

ce qui montre que ces deux opérations, communes à H_0 et H'_0, se réduisent à l'opération identique. Donc

$$\alpha' = \alpha, \qquad \beta' = \beta.$$

L'expression $S_\alpha T_\beta$ représente donc une fois et une fois seulement chaque opération de G_0. La composition de ces opérations est manifeste :

$$(S_\alpha T_\beta)(S_{\alpha'} T_{\beta'}) = (S_\alpha S_{\alpha'})(T_\beta T_{\beta'}).$$

Les opérations de G_0 se partagent ainsi naturellement en classes, telles que deux opérations d'une même classe ne diffèrent que par l'opération S de H_0. Chacune de ces classes est donc caractérisée par une opération T, et le groupe de classes ainsi formé $G_0|H_0$ est identique avec le groupe H'_0 formé des opérations T.

On verrait de même que $G_0|H'_0$ est identique à H_0.

On dit quelquefois que G_0 est le *produit* des groupes $G_0|H_0$ et H_0, c'est-à-dire de H_0 et H'_0 ; cette dénomination se comprend d'elle-même.

Nous venons de partager en classes les opérations de G_0, c'est-à-dire les *classes de première espèce* de G relatives à Γ ; cette division peut être faite directement. Deux opérations de G_0 seront d'une même classe si elles ne diffèrent que par une opération de H_0 ; donc deux substitutions de G seront d'une même *classe de seconde espèce* si elles ne diffèrent que par une substitution de H, c'est-à-dire si l'on a

$$c_\beta = ac_\alpha.$$

On déduit de là

$$c_\beta c_\alpha^{-1} = a,$$

c'est-à-dire que $c_\beta c_\alpha^{-1}$ appartient à H.

Il résulte de là que $G_0|H_0$ est identique à $G|H$; mais on a démontré que $G_0|H_0$ est holoédriquement isomorphe à H'_0, c'est-à-dire $H'|\Gamma$; on peut donc en conclure que $G|H$ *est isomorphe holoédriquement à* $H'|\Gamma$ et énoncer le résultat suivant :

Si un groupe G *possède deux sous-groupes invariants maxima* H *et* H', *si* Γ *est leur plus grand commun diviseur,* $G \mid H$ *et* $G \mid H'$ *sont respectivement isomorphes holoédriquement à* $H' \mid \Gamma$ *et* $H \mid \Gamma$, *et* $G \mid \Gamma$ *est le* PRODUIT *de* $H \mid \Gamma$ *et* $H' \mid \Gamma$.

D'ailleurs il est clair que Γ est un sous-groupe invariant *maximum* de H et de H' ; nous venons de voir en effet que $H'|\Gamma$ et $H|\Gamma$ sont holoédriquement isomorphes à $G|H$ et $G'|H$; ce sont donc des groupes *simples* ; or, il est clair que c'est là la condition pour que Γ soit un sous-groupe invariant *maximum* de H' et de H.

81. La démonstration de notre proposition :

La suite des groupes facteurs est seulement permutée lorsqu'on passe d'une suite de composition à une autre

est maintenant immédiate.

Supposons le théorème vrai pour les groupes d'ordre inférieur ou égal à N (il est évident pour les groupes d'ordre assez petit, 1 ou 2 par exemple). Nous allons le démontrer pour les groupes d'ordre au plus égal à 2N.

Soit G un groupe d'ordre au plus égal à 2N, (1) et (2) deux suites de composition de ce groupe :

$$(1) \qquad G, H, I, J, \quad \ldots, \quad M, 1,$$

$$(2) \qquad G, H', I', J', \quad \ldots, \quad M', 1.$$

Nous supposons évidemment H et H′ différents, sans quoi on commencerait à I et I′ ; soit Γ leur plus grand sous-groupe commun. On peut former les deux suites

$$(3) \qquad G, H, \Gamma, \quad \ldots, \quad 1,$$

$$(4) \qquad G, H', \Gamma, \quad \ldots, \quad 1,$$

où l'on a introduit Γ et qui sont des suites de composition de G supposées identiques à partir de Γ. D'ailleurs le théorème démontré précédemment fait voir qu'elles sont formées des mêmes groupes facteurs, puisque

$G \mid H$ est isomorphe holoédriquement à $H' \mid \Gamma$

et

$G \mid H'$ — — $H \mid \Gamma$.

Considérons maintenant les suites

$$H, I, J, \quad \ldots, \quad 1,$$

$$H, \Gamma, \quad \ldots, \quad 1;$$

l'ordre de H étant évidemment inférieur ou égal à N, ces deux suites contiennent les mêmes groupes facteurs, donc (1) et (3) conduisent au même ensemble pour ces groupes.

De même (2) et (4) conduisent également au même ensemble. Il en résulte que (1) et (2) donnent lieu aux mêmes groupes facteurs pris dans un ordre différent.

82. Nous voyons ainsi que l'étude d'un groupe quelconque se ramène à l'étude d'un certain nombre de groupes simples, *ses*

groupes facteurs ; d'ailleurs on obtient les mêmes groupes facteurs, quel que soit le procédé que l'on suive pour les former. De plus un sous-groupe invariant quelconque faisant partie d'une suite de composition du groupe, on voit qu'il n'est pas possible d'obtenir d'autre décomposition du problème que cette décomposition en groupes facteurs ; seulement si l'on ne considère pas un sous-groupe invariant maximum, plusieurs de ces groupes facteurs se trouvent encore multipliés entre eux : la décomposition est incomplète.

Le problème de la résolution des équations se ramène ainsi aux deux problèmes suivants : *décomposer un groupe en groupes facteurs ; étudier les groupes simples.* Nous étudierons d'abord, sans d'ailleurs l'approfondir, le second de ces problèmes, car il est indispensable d'avoir étudié les groupes de substitutions pour pouvoir décomposer en facteurs des groupes donnés ; de plus, nous apprendrons ainsi à connaître une classe particulièrement intéressante de groupes simples, les groupes cycliques, dont la structure est intuitive et qui sont à peu près les seuls groupes simples pour lesquels il en est ainsi. Nous pourrons alors, au lieu de considérations générales sur la décomposition d'un groupe en facteurs, étudier des problèmes particuliers, par exemple le suivant : *à quelles conditions un groupe admet-il uniquement des groupes cycliques comme facteurs ?* et nous le résoudrons dans des cas assez étendus.

III. — Groupes particuliers.

83. Dans le paragraphe précédent nous nous sommes uniquement occupés de la structure des groupes au point de vue abstrait, c'est-à-dire sans nous inquiéter de la nature intime des substitutions qui les composent ; nous allons maintenant étudier quelques groupes dont la structure, particulièrement simple, dérive facilement de la connaissance des substitutions qui les composent.

Rappelons que nous avons appelé groupe *transitif* un groupe tel qu'étant donné deux indices quelconques α et β, il renferme une substitution qui remplace α par β. Il résulte immédiatement de cette définition que *tout sous-groupe invariant d'un groupe transitif, ou*

bien se réduit à la substitution identique, ou bien déplace tous les indices. En effet, s'il déplace un indice α, il déplace un autre indice quelconque β ; car si s est la substitution qui déplace α, la transformée de s par la substitution t du groupe transitif qui remplace α par β, déplacera β ; or cette transformée est une substitution du sous-groupe, puisque celui-ci est un sous-groupe invariant.

Supposons qu'un sous-groupe invariant d'un groupe transitif soit intransitif et soient $\alpha, \beta, \gamma, \ldots, \lambda$ et $\alpha_1, \beta_1, \ldots, \lambda_1$ deux des séries d'indices que ce sous-groupe intransitif échange entre eux ; l'une des substitutions de ce sous-groupe renferme par exemple le cycle (α, β, γ) ; transformons-la par une substitution t du groupe transitif donné qui remplace α par α_1. La substitution transformée renfermera un cycle de la forme $(\alpha_1, \beta', \gamma')$; or, par hypothèse, cette substitution appartient au groupe intransitif, et les substitutions de ce groupe ne peuvent remplacer α_1 que par les indices $\beta_1, \gamma_1, \ldots, \lambda_1$; nous pouvons donc supposer que l'on a $\beta' = \beta_1$ et $\gamma' = \gamma_1$, c'est-à-dire que la substitution t remplace dans α, β, γ respectivement par $\alpha_1, \beta_1, \gamma_1$. Considérons maintenant une substitution du groupe intransitif qui échange la lettre β avec d'autres lettres que α et γ, par exemple avec δ, on verra en la transformant par la substitution t que cette substitution remplace δ par une des lettres $\delta_1, \varepsilon_1, \ldots, \lambda_1$, par exemple par δ_1, et en continuant de même on verra que la substitution t qui remplace α par α_1 remplace toutes les lettres $\alpha, \beta, \gamma, \ldots, \lambda$ par les lettres $\alpha_1, \beta_1, \ldots, \lambda_1$. Nous en concluons d'abord que le nombre des lettres de ces deux séries est le même ; de plus, ce raisonnement s'étend évidemment au cas où il y a plusieurs systèmes

$$\begin{array}{c} \alpha, \beta, \gamma, \ldots, \lambda, \\ \alpha_1, \beta_1, \gamma_1, \ldots, \lambda_1, \\ \ldots\ldots\ldots\ldots\ldots \\ \alpha_n, \beta_n, \ldots, \lambda_n, \end{array}$$

tels que le sous-groupe intransitif échange seulement entre eux les lettres de l'un des systèmes. Nous dirons que le groupe proposé est *imprimitif* et que ces divers systèmes de lettres sont *les systèmes d'imprimitivité* du groupe ; on voit que toute substitution t de ce groupe ne peut produire que les deux effets suivants : permuter en-

tre eux les indices de chacun des systèmes d'imprimitivité et permuter ces systèmes entre eux. Réciproquement, tout groupe transitif et imprimitif admet un sous-groupe invariant intransitif ; c'est le sous-groupe formé des substitutions qui ne permutent pas entre eux les divers systèmes d'imprimitivité ; il peut d'ailleurs se réduire à la substitution identique. C'est même ce dernier cas qui se présentera nécessairement lorsque le degré du groupe est un nombre premier, car alors les divers systèmes d'imprimitivité ne peuvent renfermer qu'une seule lettre. Donc *tout sous-groupe invariant d'un groupe transitif de degré premier, ou bien est transitif, ou bien se réduit à la substitution identique.*

84. Nous démontrerons enfin sur les groupes transitifs la proposition importante qui suit : *l'ordre de tout groupe transitif est un multiple de son degré.*

Soit en effet G un groupe transitif de degré quelconque m, entre les lettres $x_1, x_2, \ldots, x_m$. On peut partager les substitutions de G en m classes en rangeant dans la $k^{\text{ième}}$ classe celles qui remplacent x_1 par x_k (celles de la première classe laissant x_1 invariable). Il existe des substitutions dans chaque classe ; dans les $m-1$ dernières, parce que le groupe est transitif ; dans la première, parce que la substitution identique fait partie de tout groupe. D'autre part il est clair que si s_k désigne une substitution *déterminée* de la $k^{\text{ième}}$ classe, on obtient toutes les substitutions de la première classe, et chacune une fois seulement, en multipliant par s_k^{-1} toutes les substitutions de la $k^{\text{ième}}$ classe. Il en résulte que chaque classe renferme le même nombre de substitutions ; si on désigne ce nombre par μ, le groupe renferme $m\mu$ substitutions ; son ordre est donc un multiple de son degré m.

85. Les groupes les plus simples sont les groupes formés d'une substitution circulaire et de ses puissances ; dans le cas où la substitution circulaire déplace p indices, ils sont de degré et d'ordre égal à p ; leur structure est intuitive. D'ailleurs dans le cas où p n'est pas un nombre premier, ces groupes sont composés et sont des produits de groupes de même nature ayant pour ordre et degré les divers facteurs premiers de p. Nous pouvons donc, au point de vue qui nous intéresse, considérer seulement les grou-

pes de substitutions circulaires déplaçant un nombre premier de lettres. D'ailleurs tout groupe dont l'ordre est un nombre premier est un groupe de cette nature, car il est clair que l'ordre d'un groupe est un multiple de l'ordre de tous les cycles qui figurent dans les substitutions du groupe ; donc si un groupe est d'ordre premier p, ces substitutions ne renferment que des cycles d'ordre p ; elles peuvent d'ailleurs en renfermer plusieurs si le groupe n'est pas supposé transitif.

Nous verrons bientôt que le groupe *simple* d'ordre le moins élevé et non cyclique est d'ordre 60 ; c'est le *groupe de l'icosaèdre,* dont nous dirons quelques mots plus loin : son étude est d'ailleurs assez compliquée. On comprend dès lors l'intérêt particulier qui s'attache aux groupes cycliques et l'importance que présente la question de savoir *à quelles conditions un groupe peut être décomposé en produit de groupes cycliques*. Nous disons qu'un tel groupe est *résoluble* et que l'équation correspondante est résoluble ; il est clair en effet que lorsque cette décomposition est effectuée, la nature de l'indétermination des divers symboles définis par l'équation saute aux yeux d'une manière immédiate.

Nous allons d'abord *étudier la question* et la résoudre d'une façon complète *pour les groupes de degré premier*. Il est clair que pour qu'un groupe soit résoluble, il est nécessaire et suffisant que tous ses facteurs de composition soient des nombres premiers ; or si on a un groupe transitif de degré premier p, tous ses sous-groupes invariants sont transitifs et ont par suite pour ordre un multiple de p; donc le dernier des groupes de la série de composition a pour ordre un multiple de p ; cet ordre est d'ailleurs le facteur de composition correspondant (puisque la série de composition se termine par la substitution identique) ; donc ce dernier groupe de la série de composition est d'ordre p ; comme il est transitif c'est un groupe cyclique d'ordre p.

Le problème se trouve donc ramené au suivant : *Déterminer tous les groupes de degré p dont la série de composition se termine par une substitution circulaire d'ordre p.*

Pour résoudre ce problème il est commode d'introduire une notion nouvelle et qui acquiert en arithmétique une grande importance, celle de la *représentation analytique des substitutions.*

86. Considérons p lettres $x_1, x_2, \ldots, x_p$ (nous ne supposons pas d'abord que p soit un nombre premier ; cette hypothèse sera introduite tout à l'heure), et soit

$$\begin{pmatrix} x_1 & x_2 & \ldots & x_p \\ x_\alpha & x_\beta & \ldots & x_\lambda \end{pmatrix}$$

une substitution de ces p lettres, les lettres $\alpha, \beta, \ldots, \lambda$ ne représentent pas autre chose que les nombres $1, 2, \ldots, p$ pris dans un ordre différent. Nous savons construire une fonction $\Phi(z)$, de degré au plus égal à $p-1$, qui prend pour $z = 1, 2, \ldots, p$ les valeurs $\alpha, \beta, \ldots, \lambda$; si l'on pose en effet

$$\varphi(z) = (z-1)(z-2)\ldots(z-p),$$

l'on a

$$\Phi(z) = \frac{\alpha\varphi(z)}{(z-1)\varphi'(1)} + \frac{\beta\varphi(z)}{(z-2)\varphi'(2)} + \cdots.$$

Les coefficients de cette fonction ne sont pas nécessairement entiers; on peut, à l'aide d'une convention simple et naturelle, s'arranger pour qu'ils le soient. Les indices que nous considérons ne peuvent prendre que les valeurs $1, 2, \ldots, p$; les autres valeurs n'ayant pas de sens, nous sommes libres de leur donner tel sens qu'il nous plaira et de convenir, par exemple, que deux indices congrus suivant le module p seront considérés comme équivalents. Dès lors nous pouvons, à l'expression analytique $\Phi(z)$, qui représente des indices, ajouter ou retrancher un multiple de p et il est facile de voir, d'après les remarques faites dans la théorie élémentaire des congruences, qu'on peut ainsi s'arranger de manière que tous les coefficients soient divisibles par p. D'ailleurs la simplification peut se faire d'une manière immédiate, dans le cas où p est premier, en utilisant le théorème de Fermat et les propositions établies sur le calcul des fractions (mod. p).

On a en effet

$$\varphi(z) \equiv z^p - z \qquad (\text{mod. } p),$$

et par suite

$$\varphi'(z) \equiv -1 \qquad (\text{mod. } p),$$

d'où l'on conclut

$$\Phi(z) \equiv \varphi(z)\left[-\frac{\alpha}{z-1} + \frac{\beta}{z-2} + \cdots + \frac{\lambda}{z-p}\right] \qquad (\text{mod. } p).$$

Le polynome $\Phi(z)$ est de degré $p-1$ en z ; calculons le coefficient de z^{p-1} : c'est évidemment

$$\alpha + \beta + \cdots + \lambda = 1 + 2 + \cdots + p = \frac{p(p-1)}{2};$$

p étant un nombre premier impair, ce nombre est divisible par p ; $\Phi(z)$ est donc congru (mod. p) à un polynome de degré $p-2$ au plus. C'est là une propriété très importante des polynomes à coefficients entiers qui peuvent représenter des substitutions ; mais cette propriété ne suffit pas à les caractériser. M. Hermite a démontré une proposition plus complète : considérons une fonction $\Phi(z)$ et ses $p-2$ premières puissances ; ce sont des polynomes en z dont nous pouvons abaisser le degré au-dessous de p à l'aide de la congruence identique

$$z^p \equiv z \pmod{p}.$$

Soient $\varphi_1(z), \varphi_2(z), \ldots, \varphi_{p-2}(z)$ les polynomes de degré $p-1$ ainsi obtenus. Le théorème de M. Hermite est le suivant : *Pour que* $\Phi(z)$ *représente une substitution, il faut et il suffit que dans chacun des polynomes* $\varphi_1, \varphi_2, \ldots, \varphi_{p-2}$, *le coefficient de* z^{p-1} *soit congru à zéro* (mod. p).

Soit en effet

$$\varphi_m(z) \equiv [\Phi(z)]^m \equiv A_m + B_m z + C_m z^2 + \cdots + L_m z^{p-1} \pmod{p};$$

donnons à z les valeurs successives $1, 2, \ldots, p$ et ajoutons les relations obtenues ; on aura

$$\Sigma[\Phi(z)]^m \equiv pA_m + B_m \Sigma z + C_m \Sigma z^2 + \cdots + L_m \Sigma z^{p-1} \pmod{p}.$$

Mais les sommes $\Sigma z^i = 1^i + 2^i + \ldots + p^i$ sont toutes congrues à zéro (mod. p) tant que i est inférieur à $p-1$. Pour $i = p-1$, on a $\Sigma z^{p-1} \equiv p-1$ (mod. p), car pour z différent de p on a $z^{p-1} \equiv 1$ (mod. p) et pour $z = p$, $z^{p-1} \equiv 0$.

Il reste alors

$$\Sigma[\Phi(z)]^m = (p-1) L_m \pmod{p}.$$

D'autre part, d'après l'hypothèse faite sur $\Phi(z)$ les termes de $\Sigma[\Phi(z)]^m$ sont, à l'ordre près, ceux de la suite Σz^m, donc

$$\Sigma[\Phi(z)]^m \equiv 0 \pmod{p}.$$

On peut donc en conclure $L_m \equiv 0$ (mod. p)

pour $m = 0, 1, 2, \ldots, (p-2)$.

Réciproquement, si les coefficients $L_0, L_1, \ldots, L_{p-2}$ sont congrus à zéro suivant le module p, les expressions

$$\Sigma\Phi(z), \qquad \Sigma[\Phi(z)]^2, \ldots, \Sigma[\Phi(z)]^{p-2}$$

le seront également.

La congruence qui aura pour racines $\Phi(1), \Phi(2), \ldots, \Phi(p)$ aura donc tous ses termes nuls (mod. p) sauf le premier, et se réduira à

$$Z^p - \alpha Z \equiv 0 \qquad (\text{mod. } p).$$

Mais les racines de cette congruence satisfont aussi d'après le théorème de Fermat à la congruence

$$Z^p - Z \equiv 0 \qquad (\text{mod. } p)$$

et par suite à la congruence

$$(\alpha - 1)Z \equiv 0 \qquad (\text{mod. } p)$$

Le nombre α ne peut différer de l'unité, sans quoi le polynome $\Phi(z)$ de degré $(p-2)$ s'annulerait suivant le module p pour les p valeurs $1, 2, \ldots, p$. Donc $\alpha = 1$ et les quantités

$$\Phi(1), \Phi(2), \ldots, \Phi(p)$$

sont respectivement congrues aux nombres $1, 2, \ldots, p$.

A l'aide de ce théorème, on peut trouver aisément les fonctions $\Phi(z)$ propres à représenter une substitution ; on facilite cette recherche en remarquant que si $\Phi(z)$ représente une substitution, il en est de même de

$$\Phi(az + b) + c,$$

a, b, c étant des constantes ; ceci permet de simplifier la forme des fonctions cherchées $\Phi(z)$, en profitant des arbitraires a, b, c ; on les rétablira ensuite pour avoir la solution générale. Mais nous ne voulons pas traiter cette question intéressante et encore incomplètement étudiée ; pour plus de détails à ce sujet, nous renverrons au mémoire de M. Hermite (*Annales de Tortolini*).

87. Il est facile d'exprimer analytiquement qu'un groupe, formé des substitutions $\varphi_i(z)$ $[i = 1, 2, \ldots, r]$ reste invariant par une substitution $f(z)$; il est clair que l'on doit avoir identiquement

$$f[\varphi_i(z)] \equiv \varphi_k f(z) \qquad (\text{mod. } p),$$

i étant un indice quelconque et k dépendant de i. Proposons-nous de chercher tout d'abord un groupe admettant comme sous-groupe invariant le groupe G formé des puissances d'une substitution circulaire d'ordre p. Si on écrit cette substitution

$$(x_1, x_2, \ldots, x_p),$$

elle est représentée analytiquement par la fonction $z + 1$, ou,

suivant un usage assez général, par la notation

$$(z \mid z+1).$$

Ses puissances successives sont

$$(z \mid z+1),$$
$$(z \mid z+2),$$
$$\cdots\cdots$$
$$\cdots\cdots$$
$$(z \mid z+p-1).$$

Il s'agit de trouver dans quel groupe H ce groupe G peut être invariant ; soit $f(z)$ une substitution du groupe H ; on doit avoir, d'après une remarque faite plus haut,

$$f(z+1) = f(z) + a,$$

a ne dépendant pas de z ; en changeant successivement z en $z+1$, $z+2$, ..., $z+x$, on obtient

$$f(z+2) = f(z+1) + a = f(z) + 2a,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$f(z+x) = f(z+x-1) + a = f(z) + xa;$$

d'où, en faisant $z = 0$, $f(0) = b$:

$$f(x) = ax + b.$$

Le groupe H ne peut donc renfermer que des substitutions de la forme

$$(z \mid az+b),$$

c'est-à-dire des substitutions *linéaires*. Supposons a différent de l'unité, de manière à avoir des substitutions différentes de celles dont nous sommes partis ; il est aisé de déterminer l'ordre d'une substitution de cette forme, c'est-à-dire l'exposant de la première puissance de cette substitution qui se réduit à la substitution identique. Soit en effet

$$s = (z \mid az+b);$$

on a

$$s^2 = (z \mid a(az+b)+b) = (z \mid a^2z + ab + b).$$

De même

$$s^n = (z \mid a^nz + a^{n-1}b + a^{n-2}b + \cdots + ab + b).$$

Pour que s^n se réduise à la substitution identique, il faut et il suffit que l'on ait

$$a^n \equiv 1 \pmod{p}$$

$$b(a^{n-1} + a^{n-2} + \cdots + a + 1) \equiv 0 \pmod{p}.$$

Si, comme nous le supposons, a est différent de 1, la première congruence entraine la seconde et l'on voit que la valeur cherchée de n est l'exposant auquel appartient a relativement au nombre premier p. L'ordre des substitutions dans lesquelles a diffère de l'unité est donc inférieur à p.

Il est maintenant facile de continuer, c'est-à-dire de rechercher dans quel groupe H' le groupe H peut être invariant ; soit σ une substitution de H', la transformée par σ d'une substitution d'ordre p de H est encore d'ordre p et de plus appartient à H, puisque H est invariant ; mais nous venons de voir que les seules substitutions d'ordre p de H sont les substitutions de G ; donc G est invariant dans H' (*). Donc H' ne renferme que des substitutions linéaires. *Le groupe d'une équation résoluble de degré premier se compose donc exclusivement de substitutions linéaires.*

88. Nous allons démontrer la réciproque, en faisant voir que les facteurs de composition d'un tel groupe sont nécessairement premiers. Il est clair d'abord que toutes les substitutions linéaires $(z \mid \alpha z + \beta)$ forment un groupe et que l'ordre de ce groupe est $p(p-1)$, puisque l'on peut donner à α et β toutes les valeurs incongrues (mod. p) sous la réserve que α est différent de zéro (mod. p).

Désignons par g une racine primitive (mod. p) et par s et t les deux substitutions, d'ordres p et $p-1$,

$$(z \mid z+1), \qquad (s)$$

$$(z \mid gz). \qquad (t)$$

Il est aisé de voir que toutes les substitutions du groupe peuvent se mettre d'une manière et d'une seule sous la forme, $s^a t^b$, dans laquelle on donne à a p valeurs incongrues (mod. p) et à b, $p-1$ valeurs incongrues (mod. $p-1$). On voit ainsi une fois de plus que le groupe se compose de $p(p-1)$ substitutions distinctes.

(*) Remarquons en passant que dans une série de composition *quelconque*, chaque groupe est par définition un sous-groupe invariant du précédent, mais non de *tous* les précédents.

Pour connaître complètement la structure du groupe, il nous reste à savoir comment ces substitutions se composent entre elles.

Il suffit, pour cet objet, de vérifier l'identité

$$s^a . t^b = t^b . s^{ag^b}.$$

En effet, s^a remplace z par $z + a$, et t^b remplace $z + a$ par $g^b(z + a)$; le produit $s^a t^b$ remplace donc z par $g^b z + ag^b$; on voit de suite que $t^b s^{ag^b}$ produit le même effet.

Inversement, l'on a

$$t^b s^a = s^{ag^{p-1-b}} t^b,$$

puisque

$$g^{p-1} \equiv 1 \qquad (\text{mod. } p).$$

Il est maintenant facile de mettre sous la forme $s^a t^b$ le produit d'un nombre quelconque de substitutions données sous cette forme; l'on a immédiatement

$$s^a t^b . s^{a'} t^{b'} = s^a (t^b s^{a'}) t^{b'} = s^a s^{a' g^{p-1-b}} t^b t^{b'} = s^{a + a' g^{p-1-b}} . t^{b+b'}.$$

Le point capital à retenir, point d'ailleurs à peu près évident *a priori*, c'est que l'exposant de t dans le produit est égal à la somme des exposants de t dans les facteurs; il en résulte que, si dans un produit d'un nombre quelconque de substitutions on change l'ordre des facteurs, l'exposant de s peut seul être modifié dans le produit; celui de t reste invariable. Donc u et v désignant deux substitutions quelconques du groupe G, on a, k étant un entier déterminé,

$$uv = s^k vu,$$

ce qui peut s'écrire

$$uvu^{-1} = s^k v.$$

Donc, tout sous-groupe dont fait partie la substitution s est invariant dans le groupe G (et par suite *a fortiori* dans tous les sous-groupes de G qui le renferment); car v étant une substitution de ce sous-groupe, la transformée $s^k v$ de v par une substitution quelconque u de G en fait aussi partie.

Il suffit donc, pour montrer que les facteurs de composition de G (et aussi de tout sous-groupe de G renfermant s) sont des nombres premiers, de constater que tout sous-groupe de G renfermant s admet un sous-groupe d'indice premier (renfermant aussi s). Les sous-groupes que nous considérons renfermant tous la substitution s peuvent être classés d'après les exposants que peut avoir la substitution t dans leurs diverses substitutions. Il est clair que si

un groupe renferme la substitution t^a, il renferme toutes les substitutions de la forme t^{ma}; le nombre de celles de ces substitutions qui sont distinctes est évidemment égal au quotient de $p - 1$ par le plus grand commun diviseur de a et de $p - 1$; on en conclut qu'à tout diviseur d de $p - 1$ $(p - 1 = md)$ correspond un sous-groupe de G d'ordre mp, formé des substitutions

$$t^d, t^{2d}, \ldots, t^{md} = 1$$

et de leurs produits par les diverses puissances de s. D'ailleurs il est clair que si d' est un diviseur de d, le sous-groupe correspondant à d' renferme le sous-groupe correspondant à d. On en conclut que les facteurs de composition de G sont les facteurs premiers de $p - 1$ *dans un ordre arbitraire*, et le nombre p (*).

Donc, *pour qu'une équation irréductible de degré premier soit résoluble, il faut et il suffit que son groupe ne renferme que des substitutions de la forme*

$$(z \mid \alpha z + \beta).$$

Ces équations sont dites équations métacycliques ou équations de Galois.

89. L'étude des équations de degré composé est beaucoup plus difficile, car la représentation analytique des substitutions, qui nous a été si utile, devient moins simple; on est en effet obligé, dans le cas le plus simple où le degré de l'équation est une puissance p^ν d'un nombre premier, soit de prendre pour indices les p^ν valeurs incongrues d'une imaginaire de Galois, racine primitive de la congruence

$$i^{p^\nu} \equiv i \qquad (\text{mod. } p),$$

soit d'affecter chaque racine de ν indices, dont chacun prend p valeurs incongrues (mod. p). C'est encore plus compliqué lorsque le degré n'est pas une puissance d'un nombre premier. Aussi n'entrerons-nous pas dans cette étude, nous contentant de renvoyer aux

(*) Remarquons que, si l'on a démontré que le passage d'une série de composition à une autre permutait les facteurs de composition, on n'a nullement prouvé que toute permutation de ces facteurs pouvait être ainsi obtenue, ce qui n'est d'ailleurs pas exact; nous signalons ici l'arbitraire qui subsiste dans leur ordre, dans le cas particulier considéré.

savantes recherches de M. Jordan (*). Nous démontrerons seulement le théorème qui a servi de base à ces recherches et qui est dû à Galois ; ce théorème met d'ailleurs en évidence la constitution du groupe d'une équation résoluble, aussi tenons-nous à le donner :

Pour qu'une équation soit résoluble, il faut et il suffit qu'on puisse dériver son groupe G *d'une échelle de substitutions* 1, a, b, ... l *telles que : 1° le groupe dérivé d'un nombre quelconque des premières* 1, a, b, ..., h *soit un sous-groupe invariant de* G ; 2° *la première puissance de chacune des autres* k...l *qui soit contenue dans ce sous-groupe soit de degré premier.*

Soit N l'ordre du groupe G de l'équation ; désignons par G, H, I ... M, 1 une suite de composition de G et soient λ, μ, ..., ρ les facteurs de composition, qui sont ici des nombres premiers. Soient $h_1, h_2, \ldots, h_i$ les substitutions de H, g une substitution de G ne faisant pas partie de H, g^α la première puissance de g qui appartienne à H. Le groupe G_1 dérivé de la combinaison de g avec H aura évidemment $\alpha \cdot \frac{N}{\lambda}$ substitutions distinctes, puisque l'ordre de H est $\frac{N}{\lambda}\cdot$ Mais G_1 est contenu dans G, donc l'ordre de G_1 doit diviser l'ordre N de G, ce qui exige, puisque λ est premier, $\alpha = \lambda$.

Donc G résulte de la combinaison de H, sous-groupe invariant de G, avec g, et la première puissance de g contenue dans H est d'ordre premier λ.

On voit de même que H résulte de la combinaison d'un de ses sous-groupes invariants I avec une substitution f, telle que la première puissance de f contenue dans I soit d'ordre premier p, etc...

Réciproquement, si G résulte de la combinaison des substitutions 1, a, b, . . ., l vérifiant les conditions énoncées au théorème, on aura une suite de groupes, d'ordres

$$N, \frac{N}{\lambda}, \frac{N}{\lambda\mu}, \ldots,$$

λ, μ, ... étant premiers et chacun de ces groupes étant un sous-groupe invariant du précédent : λ, μ, ... sont donc les facteurs de composition de G, et comme ils sont premiers, l'équation correspondante sera résoluble.

(*) *Traité des Substitutions.*

90. Nous allons examiner ici le cas où le groupe de l'équation donnée est le groupe symétrique, c'est-à-dire où l'équation proposée est *générale* : nous allons chercher à déterminer la suite de composition du groupe symétrique ; nous trouverons ainsi à quelle condition l'équation générale est résoluble

Considérons donc le groupe symétrique $G_{n!}$ et désignons par H un sous-groupe invariant de $G_{n!}$. D'après la définition même d'un sous-groupe invariant, si le groupe H contient une substitution h, il contient également les transformées de h par les substitutions de $G_{n!}$, c'est-à-dire toutes les substitutions semblables à h.

Soit alors h une substitution de H ; ou bien elle renferme des cycles de plus de deux lettres, ou elle ne renferme que des cycles de deux lettres. Plaçons-nous dans le premier cas et mettons en évidence l'un des cycles de plus de deux lettres en écrivant

$$h = (\alpha_1\alpha_2\alpha_3\ldots\ldots).h',$$

h' étant une substitution des lettres qui ne figurent pas dans ce cycle.

Soient maintenant β_1, β_2, β_3 trois lettres quelconques ; considérons les deux substitutions

$$k_1 = (\beta_3\beta_1\beta_2\gamma\ldots\ldots).k,$$

$$k_2 = (\beta_3\beta_2\beta_1\gamma\ldots\ldots).k,$$

qu'on obtient en mettant d'une part au lieu de α_1, α_2, α_3 les trois lettres β_3, β_1, β_2 ou β_3, β_2, β_1, et d'autre part en remplaçant dans h toutes les autres lettres d'une manière quelconque, la même pour k_1 et k_2. Ces deux substitutions k_1 et k_2 sont par construction semblables à h ; elles appartiennent donc à H et il en est de même du produit $k_2.k_1^{-1}$ qui se réduit visiblement à la substitution circulaire $(\beta_1\beta_2\beta_3)$.

Le groupe H contient donc une substitution circulaire quelconque de trois lettres.

Plaçons-nous ensuite dans le second cas où tous les cycles de h sont de deux lettres (ou transpositions) et *supposons que n soit supérieur à quatre*.

D'abord on doit supposer que h contient plus d'un cycle, car si h contient une transposition, il les contiendra toutes et par suite sera identique à $G_{n!}$.

Soit donc $h = (\alpha_1\alpha_2)(\beta_1\beta_2).h'$, en mettant en évidence deux trans-

positions; désignons par $\gamma_1, \gamma_2, \gamma_3, \gamma_4$ quatre lettres quelconques et considérons les deux substitutions

$$k_1 = (\gamma_1\gamma_2)(\gamma_3\gamma_4)\, k,$$
$$k_2 = (\gamma_1\gamma_3)(\gamma_2\gamma_4) . k,$$

déduites de h comme il a été dit précédemment. Le groupe H contient k_1 et k_2, donc aussi $k_1 k_2^{-1} = (\gamma_1\gamma_4)(\gamma_2\gamma_3)$.

Il contient donc également la substitution

$$k_3 = (\gamma_1\gamma_5)(\gamma_2\gamma_3).$$

γ_5 étant une cinquième lettre arbitraire, et par suite le produit

$$k_1 k_2^{-1} k_3 = (\gamma_1\gamma_4\gamma_5),$$

c'est-à-dire comme précédemment une substitution circulaire de trois lettres quelconques. Nous pouvons donc affirmer que, dans tous les cas, n étant supérieur à 4 : *Tout sous-groupe invariant du groupe symétrique contient toutes les substitutions circulaires de trois lettres.*

91. Nous sommes ainsi amenés à rechercher quels groupes peuvent renfermer toutes les substitutions circulaires de trois lettres; ce qui précède montre qu'ils renferment aussi le produit de deux transpositions quelconques [on a : $(x_1x_2x_3)(x_1x_2x_4) = (x_1x_4)(x_2x_3)$] : ils renferment donc toutes les substitutions qui sont le produit d'un nombre pair de transpositions. Or, il est aisé de voir que toute substitution peut être décomposée en un produit de transpositions (pouvant avoir des lettres communes); cette décomposition est d'ailleurs possible d'une infinité de manières, mais la parité du nombre de transpositions est invariable: on peut le montrer de bien des manières (*). Considérons, par exemple, la fonction déjà étudiée

$$\begin{aligned} \delta = (x_1 - x_2)(x_1 - x_3) \ldots & (x_1 - x_n) \\ (x_2 - x_3) \ldots & (x_2 - x_n) \\ \cdot \quad \cdot \quad & \cdot \quad \cdot \quad \cdot \\ & (x_{n-1} - x_n). \end{aligned}$$

Il est facile de voir que l'effet d'une transposition est de changer

(*) Une démonstration est basée sur la division des permutations en deux classes, que l'on effectue dans la théorie élémentaire des déterminants

le signe de δ; donc une substitution se compose d'un nombre pair ou impair de transpositions suivant qu'elle laisse δ invariant ou qu'elle change son signe. On reconnaît ainsi qu'il y a $\frac{n!}{2}$ substitutions qui se composent d'un nombre pair de transpositions; elles forment un groupe dont δ est un invariant caractéristique ; ce groupe a été nommé groupe alterné et ses invariants caractéristiques sont appelés fonctions alternées. Il résulte donc de ce qui précède que : *Le seul sous-groupe invariant du groupe symétrique est le groupe alterné* ; son indice est égal à *deux*.

92. Nous connaissons déjà le premier terme de la suite des groupes que nous cherchons à former, il s'agit maintenant de rechercher les sous-groupes invariants du groupe alterné. Ceci va être très facile en appliquant un procédé analogue à celui qui nous a conduit au premier résultat.

Soit H un sous-groupe invariant de $G_{\frac{n!}{2}}$; d'abord H comme $G_{\frac{n!}{2}}$ ne pourra renfermer que des substitutions paires. Parmi toutes ses substitutions, considérons-en une de celles qui modifient le moins de lettres et décomposons-la en cycles ; dans aucun cycle il ne pourra y avoir plus de trois lettres.

Si on avait en effet $h = (\alpha_1\alpha_2\alpha_3\alpha_4 \ldots). h'$, la transformée de h par la substitution $(\alpha_2\alpha_3\alpha_4)$ qui appartient à $G_{\frac{n!}{2}}$ appartiendrait aussi à H.

Soit k cette nouvelle substitution : $k = (\alpha_1\alpha_3\alpha_4\alpha_2 \ldots). h'$; le produit $h^{-1}k = (\alpha_2\alpha_3\alpha_1 \ldots) \ldots$ appartient encore à H ; or il ne renferme plus ni α_4 ni les lettres de h', c'est-à-dire modifie moins de lettres que h, contrairement à l'hypothèse. Donc il est nécessaire que h soit composée de cycles d'au plus trois lettres.

Comme la substitution h est paire, elle renfermera un nombre quelconque de substitutions circulaires de trois lettres et un nombre pair de transpositions. On peut d'abord y supposer les transpositions disparues, car elles n'existent plus dans h^2 qui contiendrait moins de lettres que h, et qui, si h renferme une ou plusieurs substitutions circulaires, ne se réduit pas à la substitution identique.

On a donc simplement à examiner le cas où h se compose d'un

nombre pair de transpositions et celui où cette substitution consiste en permutations circulaires de trois lettres.

Soit dans le premier cas

$$h = (\alpha_1\alpha_2)(\beta_1\beta_2)\,h';$$

transformons h par la substitution $(\alpha_1\alpha_2\beta_1)$ qui appartient au groupe alterné ; nous obtenons la substitution k :

$$k = (\alpha_2\beta_1)(\alpha_1\beta_2)\,h',$$

qui appartient aussi à H ; il en est donc de même du produit $h^{-1}k$, c'est-à-dire de $(\alpha_1\beta_1)(\alpha_2\beta_2)$. Donc la substitution h ne doit contenir que deux transpositions et il est alors évident qu'en la transformant par toutes les substitutions de même forme, qui se trouvent en effet dans $G_{\frac{n!}{2}}$, on obtiendra toutes les substitutions formées de deux transpositions. Le groupe H qui doit les contenir toutes est donc identique avec le groupe alterné.

Soit de même, dans le second cas,

$$h = (\alpha_1\alpha_2\alpha_3)(\beta_1\beta_2\beta_3).\,h',$$

en supposant que h contienne au moins deux substitutions circulaires de trois lettres. Transformons h par la substitution $(\alpha_1\alpha_2\beta_1)$; nous obtenons

$$k = (\alpha_2\beta_1\alpha_3)(\alpha_1\beta_2\beta_3).\ h',$$

qui appartient à H ainsi que $kh = (\alpha_1\beta_1\beta_3\alpha_3\beta_2).\ h'^2$.

Mais cette dernière substitution contient une lettre α_2 en moins que h, donc il est nécessaire que h ne contienne qu'une substitution circulaire de trois lettres.

Soit donc $h = (\alpha_1\alpha_2\alpha_3)$ et β_1, β_2, β_3 trois lettres quelconques ; on peut transformer à l'aide d'une substitution du groupe alterné h en $(\beta_1\beta_2\beta_3)$. Il suffit en effet de transformer par la substitution

$$k = (\alpha_1\beta_1\gamma)$$

γ différant de α_1, α_2, α_3, β_1, pour obtenir $(\beta_1\alpha_2\alpha_3)$ à laquelle on appliquerait un procédé analogue. Donc le groupe H contient toutes les substitutions circulaires de trois lettres, c'est-à-dire se confond avec le groupe alterné.

Nous arrivons donc à ce résultat que le groupe alterné ne possède pas de sous-groupe invariant ; en d'autres termes : *Le groupe alterné est simple.*

Il résulte immédiatement de là que la suite de composition du

groupe symétrique de plus de quatre lettres est formée du groupe symétrique, du groupe alterné et de la substitution identique.

Le groupe alterné est d'indice premier 2 dans le groupe symétrique; mais comme l'indice de la substitution identique dans le groupe alterné est $\frac{n!}{2}$ et que ce nombre est composé, on peut dire que :

L'équation générale d'ordre n n'est pas résoluble lorsque n est supérieur à 4.

Il est facile de vérifier d'ailleurs que pour $n \leq 4$ le groupe symétrique a des facteurs de composition premiers; pour $n = 4$ on peut choisir les groupes suivants pour la série de composition :

1° le groupe symétrique, d'ordre 24;

2° le groupe alterné, d'ordre 12 et par suite d'indice 2;

3° le groupe H formé des substitutions

$$1, \quad (x_1x_2)(x_3x_4), \quad (x_1x_3)(x_2x_4), \quad (x_1x_4)(x_2x_3),$$

et par suite d'ordre 4 et d'indice 3 dans le précédent;

4° le groupe H_1 formé des substitutions

$$1, \quad (x_1x_2)(x_3x_4),$$

d'ordre 2 et d'indice 2 dans le précédent;

5° la substitution identique, d'indice 2 dans H_1.

93. On voit que le groupe *simple* qui s'offre immédiatement à nous, après les groupes cycliques, est le groupe alterné de 5 lettres; il est d'ordre $\frac{1.2.3.4.5}{2} = 60$; on le nomme groupe de l'icosaèdre parce qu'il est isomorphe au groupe des déplacements que l'on peut effectuer sur un icosaèdre régulier pour le faire coïncider avec lui-même; cette coïncidence est possible de 60 manières différentes puisque l'icosaèdre a 20 faces triangulaires et que l'on peut par suite faire coïncider une face déterminée avec une face quelconque de trois manières différentes; les déplacements qui réalisent cette coïncidence forment évidemment un groupe, lequel est d'ordre 60. Pour démontrer son isomorphisme avec le groupe alterné de 5 lettres, on remarque que les 15 droites qui joignent au centre de l'icosaèdre les milieux de ses trente arêtes forment 5 trièdres trirectangles; et que si l'on numérote ces trièdres 1, 2, 3, 4, 5, à

tout déplacement de l'icosaèdre correspond une substitution du groupe alterné effectuée sur ces numéros, et réciproquement. Nous laisserons ce point à démontrer à nos lecteurs et nous les renverrons pour plus de détails sur le groupe de l'icosaèdre à l'intéressant ouvrage de M. Klein (*). Nous avons voulu seulement donner une idée de la complication qu'atteint l'étude directe des groupes non cycliques, même dans le cas où on est aidé par une interprétation géométrique relativement simple. Nous justifions ainsi, à un point de vue purement abstrait, le nom de *résolubles* qui a été donné aux équations dont le groupe est un produit de groupes cycliques.

(*) *Vorlesungen über das Icosaeder und die Auflösung der Gleichungen vom fünften Grade.*

CHAPITRE VII

APPLICATIONS — CONCLUSION

I. — Équations normales.

94. Nous avons dans les pages qui précèdent étudié d'une manière précise la symétrie que présente l'ensemble des relations rationnelles entre les racines d'une équation irréductible quelconque ; nous avons déduit de cette étude les diverses manières de parvenir à une expression explicite de ces racines à l'aide d'autres nombres algébriques bien déterminés, c'est-à-dire les diverses manières de résoudre algébriquement l'équation. Les résultats obtenus prennent une forme particulièrement simple lorsque l'équation que l'on considère est une équation normale : il est clair, en effet, que toutes les racines d'une telle équation

$$F(z) = 0$$

s'exprimant rationnellement au moyen de l'une d'entre elles ζ, toutes leurs fonctions rationnelles sont des fonctions rationnelles de ζ ; d'où il résulte que toute réduction possible du groupe de l'équation peut être obtenue en introduisant dans le calcul des fonctions rationnelles de ζ, lesquelles sont toutes les racines d'une équation irréductible à coefficients entiers. Si l'on observe que toutes ces racines peuvent s'exprimer rationnellement à l'aide d'un nombre algébrique normal, qui en est une fonction linéaire à coefficients entiers, on en conclut qu'il suffit, pour obtenir la même réduction du groupe, d'introduire dans le calcul ce nombre algébrique normal, qui est visiblement fonction rationnelle de ζ. Nous sommes donc amenés à rechercher

les moyens de réduire le groupe d'une équation normale par l'introduction dans le calcul d'un nombre algébrique normal, fonction rationnelle de l'une de ses racines.

Nous complétons ainsi un résultat essentiel obtenu dans le Chapitre IV ; nous y avons en effet établi qu'*on doit rechercher parmi les nombres algébriques normaux les symboles-types qu'il est nécessaire d'introduire dans le calcul pour que toute équation irréductible ait un nombre de racines égal à son degré* ; on voit ici que *l'étude de la nature algébrique de chacun de ces nombres*, ou de la réduction du groupe de l'équation normale qu'il vérifie, *n'exige que la considération de nombres algébriques normaux qui en sont des fonctions rationnelles*. C'est cette étude que nous allons aborder directement.

95. Soit donc $F(z) = 0$ une équation normale irréductible de degré n, dont les coefficients peuvent même être supposés entiers, le premier d'entre eux étant l'unité ; désignons par ζ l'une de ses racines ; on obtiendra toutes ces racines,

$$\lambda_1(\zeta) = \zeta, \qquad \lambda_2(\zeta), \qquad \dots, \qquad \lambda_n(\zeta),$$

qui sont des polynomes en ζ à coefficients entiers, en décomposant dans le domaine algébrique $[\zeta]$ le polynome $F(z)$ en ses facteurs irréductibles.

Considérons alors une fonction entière de ζ à coefficients entiers $\varphi(\zeta)$; les diverses expressions $\varphi(\lambda_i(\zeta))$ peuvent être distinctes ou non : lorsqu'elles le sont, ζ peut s'exprimer à l'aide de $\varphi(\zeta)$ sous forme de polynome entier à coefficients entiers, les entiers algébriques ζ et $\varphi(\zeta)$ sont des nombres algébriques de même nature et l'étude de l'équation irréductible que vérifie $\varphi(\zeta)$ est équivalente à celle de l'équation donnée. Dans le cas contraire, le nombre p des déterminations distinctes de $\varphi(\lambda_i(\zeta))$ est un diviseur de n ; soient $n = p.q$, et

$$\varphi_1(\zeta), \qquad \varphi_2(\zeta), \qquad \dots, \qquad \varphi_p(\zeta)$$

ces déterminations distinctes ; chacune d'elles reste invariante par q transformations de la forme $[\zeta, \lambda_i(\zeta)]$, lesquelles forment nécessairement un groupe.

Ces groupes, en nombre égal à p, sont précisément ceux que nous avons nommés groupes *conjugués* dans le groupe G, formé par toutes les transformations $[\zeta, \lambda_i(\zeta)]$; on pourrait en établir ici directement les principales propriétés. Pour que l'entier algébrique $\varphi(\zeta)$ soit nor-

mal, il est nécessaire et suffisant que ces p groupes coïncident ; $\varphi(\zeta)$ est alors un invariant caractéristique d'un sous-groupe *invariant* H du groupe G. L'équation irréductible que vérifie $\varphi(\zeta)$ est de degré p et le groupe de cette équation normale est le groupe d'ordre p formé des substitutions que subit la suite $\varphi_1, \varphi_2, \ldots, \varphi_p$ par les transformations $[\zeta, \lambda(\zeta)]$.

Supposons que l'on introduise dans le calcul l'entier algébrique $\varphi(\zeta)$; le polynome $F(z)$ peut être décomposé dans le domaine algébrique ainsi obtenu en p facteurs irréductibles, tels que chacun d'eux demeure invariable par les transformations du groupe H. Ces facteurs égalés à zéro donnent visiblement des équations normales dont le groupe dans le domaine $[\varphi(\zeta)]$ est précisément H ; on passe d'ailleurs de l'une d'entre elles à toutes les autres par des transfortions $[\zeta, \lambda(\zeta)]$; il suffit par conséquent d'en étudier une seule.

Nous voyons ainsi que pour étudier une équation normale de degré pq, dont le groupe G admet un sous-groupe invariant H d'ordre q, il suffit d'étudier successivement deux équations normales : la première d'ordre p dont le groupe est le *quotient* de G par H, désigné plus haut par G | H, la seconde d'ordre q dont le groupe est le sous-groupe H lui-même.

Cette méthode de réduction peut évidemment être appliquée à chacune des deux équations normales qu'on vient d'obtenir, et l'on pourrait continuer ainsi jusqu'à ce qu'on parvienne à des équations *simples*, c'est-à-dire dont le groupe n'admet point de sous-groupe invariant. L'étude de la décomposition du groupe G, faite dans le chapitre précédent, fournit un procédé plus régulier pour obtenir le même résultat. Il est clair en effet, que si nous connaissons une suite de composition de G :

$$G,\ H,\ I,\ J,\ \ldots,\ 1,$$

il suffit de choisir le groupe H comme premier sous-groupe invariant pour que l'équation dont le groupe est G | H soit simple, d'après la définition même d'une suite de composition. Il suffira ensuite d'appliquer la méthode à l'équation dont le groupe est H ; on choisira pour cela le sous-groupe I, invariant maximum dans H, et on continuera de même.

On obtiendra donc à chaque opération *une équation normale simple* ; ces équations normales se présentent d'ailleurs dans un ordre tel

que les coefficients de chacune d'elles soient fonction entière des racines des précédentes.

Tout entier algébrique normal peut ainsi s'obtenir par l'introduction successive, dans le calcul, d'entiers algébriques normaux, racines d'équations normales simples.

On peut observer que les groupes de ces équations normales simples sont précisément les *groupes facteurs* de G; on en conclut que ces groupes sont déterminés lorsqu'on donne G et ne dépendent pas du procédé particulier employé pour les former, procédé qui ne peut faire varier que l'ordre dans lequel ils se présentent.

L'étude d'un domaine algébrique quelconque se trouve ainsi ramenée à l'étude successive d'un certain nombre d'équations *normales simples*, dont les groupes sont fixés lorsqu'on donne le domaine.

96. Nous venons de voir que, dans le cas des équations normales, à toute réduction du groupe correspond une décomposition de l'équation en facteurs, exactement équivalente. Il n'en est pas toujours de même dans le cas général; il peut arriver que l'introduction dans le calcul d'un nombre algébrique réduise le groupe d'une équation non normale, sans pour cela la rendre réductible; nous allons préciser les conditions dans lesquelles un tel fait peut se produire. Il est clair qu'une équation irréductible ne peut devenir réductible que si son groupe est réduit à l'un de ses sous-groupes invariants *intransitifs*. Or nous avons vu (83) que lorsqu'un groupe G admet un sous-groupe invariant intransitif, G est imprimitif. La décomposition en facteurs d'une équation ne pourra donc se produire que lorsqu'il se trouve dans l'une des suites de composition de son groupe, un groupe imprimitif. Nous allons voir d'ailleurs que dans ce cas, on peut effectivement réaliser cette décomposition.

Étudions en effet la résolution des équations à groupe imprimitif; désignons par $\lambda\mu$ le degré de l'équation et supposons que ses racines se classent en λ systèmes d'imprimitivité, comprenant chacun μ racines :

$$\begin{array}{l} x_1,\ x_2,\ \ldots,\ x_\mu, \\ y_1,\ y_2,\ \ldots,\ y_\mu, \\ \ldots\ldots\ \ldots\ldots \\ v_1,\ v_2,\ \ldots,\ v_\mu, \end{array}$$

le nombre des lettres $x, y, \ldots, v$ étant égal à λ. Par hypothèse le groupe G de l'équation se compose de substitutions de la forme st, les substitutions s portant sur les indices $1, 2, \ldots, \mu$ des lettres $x, y, \ldots, v$ et les substitutions t permutant entre elles ces lettres $x, y, \ldots, v$ sans toucher à leurs indices ; les substitutions s forment d'ailleurs un groupe S de degré μ et les substitutions t un groupe T de degré λ : l'ordre de G est égal au produit des ordres des groupes S et T, ordres que nous désignerons par σ et τ.

Soit X une fonction symétrique quelconque des lettres

$$x_1, x_2, \ldots, x_\mu,$$

Y la même fonction symétrique des lettres

$$y_1, y_2, \ldots, y_\mu,$$

etc..., V la même fonction symétrique des lettres v.

Il est clair que la fonction

$$\varphi(z) = (z - \mathrm{X})(z - \mathrm{Y}) \ldots (z - \mathrm{V})$$

reste invariable par les substitutions du groupe G ; elle s'exprime donc rationnellement au moyen des coefficients de l'équation proposée ; c'est-à-dire que les expressions X, Y, ..., V sont racines d'une équation de degré λ à coefficients rationnels. Il est facile de voir que le groupe de cette équation est précisément le groupe T, car les fonctions rationnelles de ses racines invariables par les substitutions de T sont précisément les fonctions rationnelles des racines de la proposée invariable par les substitutions de G.

D'autre part, d'après ce que nous avons vu plus haut, il est toujours possible de choisir la fonction symétrique X de manière que toutes les fonctions symétriques des x s'expriment rationnellement au moyen de X ; dès lors les fonctions symétriques des y s'expriment rationnellement *de la même manière* au moyen de Y, etc. On en conclut que l'on a :

$$(x - x_1)(x - x_2) \ldots (x - x_\mu) = \mathrm{F}(x, \mathrm{X}),$$

$$(y - y_1)(y - y_2) \ldots (y - y_\mu) = \mathrm{F}(y, \mathrm{Y}),$$

. . . .

$$(v - v_1)(v - v_2) \ldots (v - v_\mu) = \mathrm{F}(v, \mathrm{V}),$$

en désignant par $\mathrm{F}(x, \mathrm{X})$ une fonction entière de x et de X ; d'ailleurs lorsqu'on adjoint X, le groupe de l'équation

$$\mathrm{F}(x, \mathrm{X}) = 0$$

est précisément le groupe S ; on le voit comme précédemment.

On conclut immédiatement de là que l'équation proposée peut s'écrire

$$F(\xi, X)F(\xi, Y) \dots F(\xi, V) = 0.$$

Son premier membre est le résultant des premiers membres des équations

$$(\alpha) \begin{cases} \varphi(z) = 0, \\ F(\xi, z) = 0; \end{cases}$$

la première de ces équations est de degré λ et son groupe est d'ordre τ ; la seconde est de degré μ et son groupe d'ordre σ.

La réciproque de cette proposition est immédiate : toute équation résultant d'un tel calcul a son groupe imprimitif et constitué comme nous venons de le voir au moyen des groupes des équations (α).

II. — Équations abéliennes.

97. Nous avons appelé groupe *abélien* un groupe dont les substitutions sont échangeables entre elles ; il résulte de cette définition que tout sous-groupe d'un groupe abélien en est nécessairement un sous-groupe invariant. On peut prévoir que cette propriété simplifiera l'étude de la structure du groupe et l'on est ainsi amené à considérer une classe importante d'équations normales, celles dont le groupe est un groupe abélien.

Les résultats acquis dans le paragraphe précédent relativement au groupe d'une équation normale nous permettent alors de dire qu'une équation irréductible

$$f(x) = 0,$$

est *abélienne* lorsque : 1° ses racines s'expriment en fonction rationnelle de l'une d'elles x_1, c'est-à-dire que l'on a

$$x_2 = \varphi_2(x_1), \qquad x_3 = \varphi_3(x_1), \dots ;$$

2° les fonctions φ définies par les égalités précédentes vérifient les relations

$$\varphi_\alpha[\varphi_\beta(x_1)] = \varphi_\beta[\varphi_\alpha(x_1)].$$

Il importe de remarquer que l'on n'a pas nécessairement d'une façon identique

$$\varphi_\alpha[\varphi_\beta(x)] = \varphi_\beta[\varphi_\alpha(x)] ;$$

il suffit que cette égalité ait lieu lorsqu'on remplace x par une racine x_1 de l'équation considérée.

La définition précédente pourrait s'étendre à des équations réductibles, mais nous allons montrer que l'on peut se contenter d'étudier les équations abéliennes irréductibles, car *les facteurs irréductibles d'une équation abélienne sont des équations abéliennes.*

Soit
$$F(x) = 0$$
une équation abélienne. Nous désignerons par $f_1(x)$ et $f_2(x)$ deux facteurs irréductibles de F, en supposant par exemple que x_1 soit racine de l'équation
$$f_1(x) = 0.$$

L'équation $f_1(x) = 0$ admet les racines $x_1, \varphi(x_1), \ldots$; elle est donc manifestement abélienne.

Une racine de l'autre équation $f_2(x) = 0$ est alors de la forme $\theta(x_1)$, et dans ce cas les deux équations
$$f_1(x) = 0,$$
$$f_2[\theta(x)] = 0$$
ont une racine commune x_1. L'équation $f_2[\theta(x)] = 0$ admet donc toutes les racines de $f_1(x)$, c'est-à-dire $\varphi(x_1)$, $\psi(x_1) \ldots$; si l'on pose
$$\theta(x_1) = x_2$$
les racines de $f_2(x)$ qui s'écrivent
$$\theta(x_1), \quad \theta[\varphi(x_1)], \quad \theta[\psi(x_1)] \ldots .$$
seront
$$x_2, \quad \varphi(x_2), \quad \psi(x_2), \ldots$$
à cause des relations de la forme
$$\theta[\varphi(x_1)] = \varphi[\theta(x_1)].$$

D'autre part ces racines vérifient des relations analogues ; on a, par exemple,
$$\varphi[\psi(x_2)] = \psi[\varphi(x_2)].$$

Cette relation peut en effet se déduire de la suite d'égalités
$$\varphi\Big[\psi\{\theta(x_1)\}\Big] = \varphi\Big[\theta\{\psi(x_1)\}\Big] = \psi\Big[\varphi\{\theta(x_1)\}\Big].$$

Il reste à montrer que l'on obtient ainsi toutes les racines de $f_2(x)$; pour le voir, considérons le produit
$$[x - \theta(x_1)][x - \theta[\varphi(x_1)]][x - \theta[\psi(x_1)]] \ldots$$

étendu à toutes les racines de l'équation

$$f_1(x) = 0\ ;$$

c'est une fonction symétrique des racines de cette équation ; elle s'exprime donc rationnellement au moyen de ses coefficients; or d'après ce que nous venons de voir, l'équation obtenue en l'égalant à zéro admet une racine de l'équation

$$f_2(x) = 0;$$

son premier membre est donc divisible par $f_2(x)$ puisque ce polynome est irréductible.

98. Nous pouvons donc nous borner à l'étude des équations abéliennes irréductibles. Soit

$$f(x) = 0$$

une telle équation, x_1 une de ses racines ; les autres racines sont de la forme

$$\varphi(x_1), \quad \psi(x_1), \ \ldots, \ \varpi(x_1).$$

Les transformations $[x_1, \varphi(x_1)]$, $[x_1, \psi(x_1)]$, ..., $[x_1, \varpi(x_1)]$ sont toutes les transformations distinctes d'un groupe qui est précisément isomorphe holoédriquement au groupe de l'équation $f(x) = 0$. Nous allons mettre en évidence la structure de ce groupe, c'est-à-dire celle d'un groupe abélien quelconque. Nous observerons pour cela, en désignant par $\Theta(x_1)$ l'une quelconque des racines de $f(x)$, que si la transformation $[x_1, \Theta(x_1)]$ est d'ordre n, c'est-à-dire si le groupe formé par ses puissances est d'ordre n, et si l'on a $n = p.q$, la transformation $[x_1, \Theta^q(x_1)]$ est d'ordre p. Si l'on considère également deux transformations $[x_1, \varphi(x_1)]$ et $[x_1, \psi(x_1)]$ dont les ordres respectifs a et b sont premiers entre eux, la transformation $[x_1, \varphi[\psi(x_1)]]$ est d'ordre égal à ab.

Il résulte de là que si nous désignons par a, b, ..., l les ordres respectifs des transformations correspondant à φ, ψ, ..., ϖ, et par m_1 leur plus petit commun multiple, qui décomposé en facteurs premiers peut s'écrire $m_1 = p^\alpha q^\beta \ldots$, l'on peut former une transformation du groupe dont l'ordre est m_1. En effet, p^α est diviseur de l'un au moins des nombres a, b, ... ; supposons par exemple que l'on ait $a = p^\alpha.a'$, la transformation qui correspond à $\varphi^{a'}(x_1)$ est d'ordre p^α ; si l'on a de même $b = q^\beta.b'$, la transformation cor-

respondant à $\psi^{\beta'}(x_1)$ sera d'ordre égal à q^{r}, etc.... La transformation $[x_1, \Theta_1(x_1)]$, où l'on a posé

$$\Theta = \varphi^{\beta}\psi^{\beta'}\dots,$$

sera évidemment une transformation répondant à la question.

Soit N le degré de l'équation $f(x) = 0$; si l'on a $m_1 = N$, toutes les racines de l'équation figurent et figurent une fois seulement dans la suite

$$x_1, \Theta_1(x_1), \Theta_1^2(x_1), \dots, \Theta_1^{m_1-1}(x_1);$$

dans ce cas le groupe G des transformations qu'admet l'équation $f(x) = 0$ est formé des puissances d'une seule transformation $[x, \Theta_1(x)]$, et le groupe de l'équation est formé de toutes les puissances d'une même substitution : celle qu'éprouvent les éléments de la suite

$$x_1, \varphi(x_1), \psi(x_1), \dots, \varpi(x_1)$$

lorsqu'on y remplace x_1 par $\Theta_1(x_1)$.

Lorsque m_1 n'est pas égal à N, il en est un diviseur et les puissances de la transformation $[x_1, \Theta_1(x_1)]$ forment un sous-groupe H_1 de G, nécessairement invariant ; les transformations de G peuvent donc être partagées en *classes* telles que deux transformations d'une même classe puissent s'écrire sous la forme

$$[x_1, \psi_1(x_1)] \quad \text{et} \quad [x_1, \Theta_1^{\alpha}\psi_1(x_1)],$$

c'est-à-dire ne diffèrent que par une transformation de H_1. Choisissons dans chaque classe une transformation, et soient $a_1, b_1, \dots,$ les ordres respectifs de ces transformations ; ces ordres sont compris dans la suite $a, b, \dots,$ c'est-à-dire sont des diviseurs de m_1 ; nous savons former une transformation

$$[x_1, \Theta_2(x_1)],$$

dont l'ordre est égal au plus petit multiple commun m_2 des nombres $a_1, b_1, \dots,$ qui est aussi un diviseur de m_1.

Si l'on considère alors les expressions

$$\Theta_1^{\alpha_1}\Theta_2^{\alpha_2}(x_1),$$

α_1 et α_2 prenant respectivement toutes les valeurs entières inférieures à m_1 et à m_2, elles sont distinctes et représentent par conséquent m_1m_2 racines de l'équation $f(x) = 0$.

Lorsqu'on n'a pas obtenu ainsi toutes les racines de cette équation, c'est-à-dire lorsqu'on n'a pas $m_1m_2 = N$, on recommence le

partage en classes des transformations de G en partant du sous-groupe H_2 engendré par toutes les transformations qui correspondent aux racines déjà obtenues. Il est clair qu'*on parvient ainsi à mettre toutes les racines de l'équation donnée sous la forme*

$$\Theta_1^{\alpha_1}\Theta_2^{\alpha_2} \ldots \Theta_\mu^{\alpha_\mu}(x_1),$$

où l'on a
$$\alpha_i = 0, 1, \ldots, (m_i - 1),$$
$$(i = 1, 2, \ldots, \mu),$$

et où les entiers $m_1, m_2, \ldots m_\mu$ ont pour produit N, chacun d'eux étant d'ailleurs diviseur du précédent.

99. L'expression que nous venons d'obtenir pour les racines de l'équation abélienne $f(x) = 0$, conduit aisément à la résolution algébrique de cette équation. Nous commencerons par examiner le cas où toutes ses racines peuvent se mettre sous la forme

$$x_1, \Theta(x_1), \Theta^2(x_1), \ldots, \Theta^{m_1-1}(x_1),$$

c'est-à-dire où toutes les transformations qu'elle admet sont les puissances de l'une d'entre elles.

Le groupe de l'équation est formé des m_1 puissances de la substitution qu'éprouvent ces racines lorsqu'on y remplace x_1 par $\Theta(x_1)$, c'est-à-dire des puissances de la substitution circulaire

$$\left(x_1, \Theta(x_1), \ldots, \Theta^{m_1-1}(x_1)\right).$$

Si le nombre m_1 est premier, ce groupe est simple : l'équation est de celles que nous avons appelées résolubles : *sa résolution consiste pour nous dans l'expression de ses racines sous la forme*

$$x_1, \Theta(x_1), \ldots, \Theta^{m_1-1}(x_1)$$

avec la relation

$$\Theta^{m_1}(x_1) = x_1.$$

Dans le cas où le nombre m_1 n'est pas premier, le groupe est composé : ses groupes facteurs sont des groupes cycliques ayant pour ordres les divers facteurs premiers — égaux ou inégaux — de m_1 : la résolution de l'équation se ramène alors à la résolution successive d'équations analogues, mais dont le degré est premier.

Réciproquement, si le groupe d'une équation est cyclique, c'est-à-dire formé des puissances d'une substitution circulaire, l'équation appartient à la classe de celles que nous venons d'étudier et il est facile de trouver la fonction Θ. Désignons en effet par $x_1, x_2, \ldots, x_m$

ses racines et par

$$(x_1, x_2, \ldots, x_m)$$

la substitution circulaire dont les puissances forment le groupe de l'équation ; en posant

$$f(x) = (x - x_1)(x - x_2)\ldots(x - x_m)$$

et

$$\Theta(x) = \frac{x_2 f(x)}{(x - x_1)f'(x_1)} + \frac{x_3 f(x)}{(x - x_2)f'(x_2)} + \cdots + \frac{x_1 f(x)}{(x - x_m)f'(x_m)},$$

la fonction $\Theta(x)$ reste invariable par les substitutions du groupe de l'équation, c'est donc une fonction rationnelle de x ; on a de plus

$$\Theta(x_1) = x_2, \Theta(x_2) = x_3, \ldots, \Theta(x_{m-1}) = x_m, \Theta(x_m) = x_1,$$

ce qui démontre la proposition énoncée.

100. Nous allons supposer maintenant le nombre μ supérieur à l'unité ; pour fixer les idées nous le prendrons égal à *trois*, mais les raisonnements s'étendront visiblement au cas général. Les racines de l'équation sont par conséquent comprises dans la formule

$$\Theta_1^{\alpha_1}\Theta_2^{\alpha_2}\Theta_3^{\alpha_3}(x_1),$$

avec

$$\alpha_1 = 1, 2, \ldots, m_1,$$
$$\alpha_2 = 1, 2, \ldots, m_2,$$
$$\alpha_3 = 1, 2, \ldots, m_3;$$

on a d'ailleurs

$$\Theta_1^{m_1}(x_1) = \Theta_2^{m_2}(x_1) = \Theta_3^{m_3}(x_1) = x_1.$$

Considérons les fonctions symétriques des $m_2 m_3$ racines

$$(1) \qquad \Theta_1^{a}\Theta_2^{\alpha_2}\Theta_3^{\alpha_3}(x_1),$$

$$\alpha_2 = 1, 2, \ldots, m_2; \qquad \alpha_3 = 1, 2, \ldots, m_3,$$

dans lesquelles a désigne un entier fixe. Ces diverses fonctions symétriques s'expriment rationnellement au moyen d'une quelconque d'entre elles, puisque ce sont des invariants d'un même groupe : le groupe qui correspond aux transformations

$$[x_1, \Theta_2^{\alpha_2}\Theta_3^{\alpha_3}(x_1)].$$

Soit φ_a l'une quelconque de ces fonctions symétriques : $\varphi_1, \varphi_2, \ldots, \varphi_{m_1}$, les expressions qu'on déduit de φ_a en y remplaçant successivement a par $1, 2, \ldots, m_1$; ce sont les fonctions conjuguées de φ_a dans le groupe de l'équation, et on voit immédiatement que la trans-

formation $[x_1, \theta_1(x_1)]$ leur fait éprouver la substitution circulaire

$$S_1 = (\varphi_1, \varphi_2, \ldots, \varphi_{m_1}),$$

les transformations $[x_1, \theta_2(x_1)]$ et $[x_1, \theta_3(x_1)]$ les laissant invariables. Par suite une transformation quelconque du groupe fait éprouver aux fonctions φ la substitution S_1 ou l'une de ses puissances. Ces fonctions sont donc racines d'une équation irréductible d'ordre m_1 à coefficients rationnels, dont le groupe est cyclique. Si l'on adjoint une racine φ de cette équation, toutes les fonctions symétriques des éléments

$$\theta_1^a \theta_2^{\alpha_2} \theta_3^{\alpha_3}(x_1),$$

$$\alpha_2 = 1, 2, \ldots, m_2, \qquad \alpha_3 = 1, 2, \ldots, m_3,$$

s'expriment rationnellement à l'aide de φ, quel que soit a. Nous considérerons maintenant les fonctions symétriques des racines

$$\theta_1^a \theta_2^b \theta_3^{\alpha_3}(x_1),$$

$$\alpha_3 = 1, 2, \ldots, m_3,$$

a et b étant des entiers fixes. La même méthode montrera, que, ψ_b étant l'une de ces fonctions symétriques et $\psi_1, \psi_2, \ldots, \psi_{m_2}$ celles qui s'en déduisent en remplaçant b par $1, 2, \ldots m_2$, ces fonctions ψ sont les racines d'une équation irréductible de degré m_2, à coefficients rationnels en φ, dont le groupe est cyclique. Toutes les fonctions symétriques considérées (a et b étant quelconques) s'expriment d'ailleurs rationnellement au moyen d'une racine ψ de cette équation.

On verra enfin, par un raisonnement analogue, que les diverses expressions

$$\theta_1^a \theta_2^b \theta_3^c(x_1),$$

c'est-à-dire les racines de l'équation proposée, s'expriment rationnellement au moyen d'une racine d'une équation irréductible de degré m_3 dont le groupe est cyclique et dont les coefficients sont rationnels en φ et en ψ.

Nous établissons ainsi directement que les équations abéliennes sont résolubles et les calculs que nous venons d'indiquer équivalent à une décomposition de tout groupe abélien en *facteurs*. Chacun des groupes cycliques d'ordres m_1, m_2, m_3 est en effet le produit de groupes cycliques d'ordre premier, c'est-à-dire de groupes simples. Cette décomposition du groupe en facteurs résulterait d'ail-

leurs immédiatement du fait que, si l'on pose $m = pq$, les transformations

$$(x_1,\ \Theta_1^{hp}\Theta_2^{\alpha_2}\Theta_3^{\alpha_3}x_1),$$

$$h = 1, 2, \ldots, q, \qquad \alpha_2 = 1, 2, \ldots, m_2, \qquad \alpha_3 = 1, 2, \ldots, m_3,$$

en forment un sous-groupe invariant d'indice p et qu'on peut toujours prendre pour p un nombre premier. On trouvera, en effet, par la même méthode un sous-groupe invariant d'indice premier du sous-groupe obtenu, et ainsi de suite.

On voit de plus, par cette marche, que l'ordre dans lequel se présentent les facteurs de composition peut être choisi arbitrairement dans le cas particulier d'un groupe abélien.

101. Nous ne voulons pas terminer sans signaler parmi les équations abéliennes celles qui ont la forme $x^n - 1 = 0$, où n est un entier quelconque, et donc les facteurs irréductibles sont des équations cycliques. L'étude de ces équations, faite par Gauss, a été l'origine de travaux qui ont illustré Kummer et Kronecker et qui se rattachent aux théories les plus profondes de l'Algèbre et de l'Analyse ; pour plus de détails, nous renverrons le lecteur à l'excellente monographie de M. Bachmann : *Die Lehre von der Kreistheilung*.

Faisons enfin observer que l'équation $x^p - A = 0$, où p est premier et où A n'est pas la puissance $p^{\text{ième}}$ d'un nombre rationnel appartient à la classe des équations métacycliques et devient abélienne par l'introduction d'une racine de l'équation

$$x^{p-1} + x^{p-2} + \cdots + x + 1 = 0.$$

On sait que l'on introduit d'habitude dans les éléments un signe particulier, $\sqrt[p]{A}$, pour représenter une racine de cette équation. Cette notation n'a d'ailleurs aucune importance au point de vue où nous nous sommes placés et n'avance en rien la résolution algébrique de l'équation. Il est néanmoins indispensable de signaler que les racines des équations que nous avons appelées résolubles peuvent toujours s'obtenir par la résolution successive d'équations binomes ; en d'autres termes, ces équations sont *résolubles par radicaux*. C'est d'ailleurs ce problème de la résolution par radicaux qui a été l'origine première des recherches fondamentales de Lagrange, Abel et Galois.

CONCLUSION

Nous terminons ici les développements que nous avions l'intention de donner à l'Algèbre ; peut-être ne sera-t-il pas mauvais de résumer rapidement les résultats obtenus, en mettant en évidence la marche suivie pour y parvenir.

Après avoir défini les entiers positifs comme des *signes* ou *symboles* se combinant entre eux suivant certaines lois qui nous ont été suggérées par la considération des systèmes d'unités, nous leur avons rattaché les entiers négatifs et les nombres fractionnaires en conservant pour ces nouveaux symboles les mêmes lois de combinaison et en liant chacun d'eux aux symboles déjà connus par une relation qui lui sert de définition. Nous avons fait ainsi un certain nombre d'hypothèses et, comme les propriétés bien connues des entiers positifs ont montré immédiatement qu'elles n'étaient point contradictoires, nous n'avons pas cherché à les réduire au nombre minimum. Il serait facile d'ailleurs de procéder en ne faisant jamais que des hypothèses indispensables :

Les entiers positifs seront, par exemple, les symboles déduits de l'un d'entre eux, le nombre un, par une composition répétée de ce symbole avec lui-même, cette composition possédant les quatre propriétés attribuées à l'addition : il est clair en effet que ces hypothèses sont nécessaires et suffisantes pour construire pour ces symboles une table carrée d'addition. Le nombre zéro sera un nouveau symbole d'effet nul dans sa composition par addition avec lui-même ou avec tout nombre entier. Les entiers négatifs seront tous les symboles qui se composant entre eux et avec les entiers en suivant les lois de l'addition vérifient des relations de la forme $a+x=0$, où a désigne un entier positif. On montre qu'il est possible de trouver entre ces symboles un second mode de composition qui possède les propriétés de la multiplication des entiers positifs de sorte que le calcul additif et multiplicatif est complètement défini pour l'ensemble des entiers positifs et négatifs.

Les nombres rationnels seront enfin tous les symboles qui, possédant entre eux et avec les entiers positifs ou négatifs un mode de

composition admettant les quatre propriétés de la multiplication, vérifient des relations de la forme $a.x = 1$, où a désigne un entier positif ou négatif, et tous les symboles qui résultent de la composition de ces derniers entre eux et avec les entiers par le mode considéré. On établit qu'il est possible de définir un second mode de composition de ces symboles entre eux lié à la multiplication de la même manière que l'addition pour les entiers et qui possède les propriétés de l'addition des entiers : le calcul additif et multiplicatif est ainsi complètement défini pour l'ensemble des entiers positifs et négatifs et des nombres rationnels.

Nous avons procédé de même pour introduire dans le calcul les nombres algébriques qui sont pour nous tous les symboles x qui, se composant entre eux par addition et par multiplication en suivant les mêmes lois que les entiers, vérifient des relations de la forme

$$(1) \qquad f(x) = 0,$$

où $f(x)$ désigne un polynome irréductible. On établit d'abord que s'il existe effectivement un symbole satisfaisant à ces conditions, il existe pour ce polynome un nombre de symboles possédant ces propriétés égal à son degré n. Ces symboles vérifient nécessairement les relations

$$(2) \qquad S_1 = p_1, \qquad S_2 = p_2, \qquad \ldots, \qquad S_n = p_n,$$

où $S_1, S_2, \ldots, S_n$ désignent leurs fonctions symétriques élémentaires et $p_1, p_2, \ldots, p_n$ les coefficients du polynome $f(x)$ et inversement, il suffit que ces relations soient vérifiées par les symboles $x_1, x_2, \ldots, x_n$ pour que $f(x)$ s'annule pour $x = x_1$, $x = x_2$, ..., $x = x_n$. On est ainsi amené à rechercher toutes les conséquences de ces relations en partant des propriétés attribuées à nos symboles et c'est dans cette substitution des relations (2) à la relation (1) que réside, ainsi que l'a fait remarquer Kronecker, la différence essentielle entre le point de vue de Galois et celui auquel s'est toujours placé Abel.

La recherche de toutes les conséquences de relations plus générales :

$$F_1 = 0, \qquad F_2 = 0, \ldots, \qquad F_m = 0,$$

entre des symboles $x_1, x_2, \ldots, x_n$ possédant les modes de composition indiqués, nous conduit à partager dans le cas où elles sont

« compatibles » (*) les systèmes de telles relations en *réductibles* ou *irréductibles*, suivant qu'il existe ou non de nouvelles relations entre les mêmes symboles qui ne sont point des conséquences nécessaires des premières ; c'est là qu'il faudra chercher la raison de la différence signalée plus loin entre les équations *générales* et les équations spéciales. Il résulte d'ailleurs de la considération de la *résolvante générale*, dont l'introduction est due à Liouville, que toutes les hypothèses faites sur $x_1, x_2, \ldots, x_n$, lorsqu'elles sont « compatibles », équivalent à supposer qu'un symbole ζ possédant les mêmes modes de composition vérifie une relation de la forme $R(\zeta) = 0$, où $R(z)$ désigne un polynome irréductible déterminé. Le calcul de tels symboles est simplement un calcul de polynomes en ζ, [mod. $R(\zeta)$], c'est-à-dire un calcul où l'on néglige les multiples de $R(\zeta)$, et à ce titre il est visible qu'il ne peut renfermer de contradiction, ce qui établit la possibilité logique de définir $x_1, x_2, \ldots, x_n$ comme nous l'avons fait.

Il suffit d'établir que les relations

$$(2) \qquad S_1 = p_1, \qquad S_2 = p_2, \ldots, \qquad S_n = p_n,$$

sont toujours « compatibles » au sens attribué à ce mot, pour en conclure la possibilité logique de définir les nombres algébriques, et l'on parvient ainsi en même temps aux propositions essentielles dues à Galois et relatives à la symétrie de l'ensemble des relations rationnelles qui existent entre les racines $x_1, x_2, \ldots, x_n$ de l'équation $f(x) = 0$.

Signalons en passant l'importance, plusieurs fois mise en évidence, du fait qu'il existe pour représenter toute fonction symétrique de $x_1, x_2, \ldots x_n$ une forme *unique* ne dépendant que des fonctions symétriques élémentaires.

Une étude générale des divers genres de symétrie qui peuvent se présenter — théorie des groupes de substitutions (**) — montre de quelle nature sont les relations qui lient entre elles les diverses fonctions rationnelles de n indéterminées, et les théorèmes de Lagrange donnent le moyen de former effectivement ces relations ; il est aisé

(*) Le mot « compatibles » a ici un sens parfaitement défini, pour lequel nous renvoyons au § 42.

(**) Nous avons naturellement adopté dans cette théorie les notations introduites dans la théorie plus générale des Groupes de Transformations par son créateur, le célèbre géomètre norwégien Sophus Lie.

d'indiquer alors comment ces résultats doivent être modifiés lorsqu'on choisit pour les x, les racines de l'équation déterminée $f(x) = 0$.

La considération qui vient ensuite de l'ensemble des relations rationnelles entre les racines $x_1, x_2, \ldots, x_n$ de l'équation

$$f(x) = 0$$

et les racines $y_1, y_2, \ldots, y_p$ d'une autre équation quelconque

$$g(y) = 0$$

permet d'établir qu'on ne parvient de cette manière à aucune espèce de symétrie qui ne soit aussi obtenue en prenant pour $y_1, y_2, \ldots, y_p$ des fonctions rationnelles convenablement choisies des x ; quelques propositions sur les groupes de substitutions montrent comment on parvient à la symétrie la plus générale en partant de symétries particulières données par des groupes *simples*, et l'interprétation de ces propositions à l'aide des nombres algébriques constitue la théorie de la résolution algébrique des équations.

Nous avons donné ensuite quelques exemples de symétries particulièrement faciles à saisir telles que celles données par des produits de groupes cycliques, qui correspondent aux équations dites *résolubles* et celles relatives aux équations du quatrième et du cinquième degré ; nous avons montré en passant que *l'équation générale d'ordre supérieur à quatre n'est pas résoluble*, proposition qui a occupé longtemps les géomètres et dont la première démonstration entièrement rigoureuse est due à Abel.

Un dernier chapitre est consacré à l'étude directe d'une classe importante de nombres algébriques au moyen desquels tous les autres s'expriment rationnellement : les nombres algébriques *normaux*. Parmi ceux-là on peut encore signaler ceux qui sont définis par une équation dont le groupe est *abélien*, c'est-à-dire dont le groupe a ses substitutions échangeables, et l'on établit que tout groupe de cette nature est *résoluble*, c'est-à-dire est un produit de groupes cycliques.

Nous avons sans doute laissé dans l'ombre une foule de questions intéressantes ; nous espérons néanmoins que ce que nous avons fait suffira pour inspirer au lecteur le désir d'une étude plus approfondie et nous le renverrons en particulier pour cela aux divers ouvrages que nous avons consultés et dont nous donnons ici la liste :

E. GALOIS : *Œuvres mathématiques*, Journal de Liouville, 1846.

J. LIOUVILLE : *Mémoire sur la théorie de l'élimination dans les équations algébriques*. Journal de Liouville, 1841.

C. JORDAN : *Traité des substitutions*, 1870.

L. KRONECKER : *Grundzüge einer arithmetischen Theorie der algebraischen Grœssen*. Journal de Crelle, t. 92, 1880.

J. A. SERRET : *Cours d'Algèbre supérieure*, 5e édition 1885.

E. NETTO : *Substitutionentheorie*, 1882.

J. MOLK : *Sur une notion qui comprend celle de la divisibilité et sur la théorie générale de l'élimination*, Acta Mathematica, t. 6.

O. BOLZA : *On the Theory of Substitution-Groups and its Applications to Algebraic Equations*, American Journal of Mathematics, t. XIII.

NOTES

NOTE I

SUR LE THÉORÈME DE FERMAT

Comme nous l'avons remarqué (§ 5), le théorème de Fermat nous fournit un exemple d'une congruence suivant un module premier p qui, sans être identique, est vérifiée pour toute valeur entière de la variable. En d'autres termes, *le polynome* $x^p - x$ *est divisible par le nombre premier* p, *quel que soit l'entier* x, *sans que les coefficients de ce polynome soient divisibles par* p. Il est clair d'ailleurs que les polynomes divisibles (*) par $x^p - x$ jouissent de cette même propriété, à l'exclusion de tous les autres. Le théorème de Fermat apparait ainsi, comme un exemple unique de ce qu'on peut appeler *la divisibilité d'un polynome par un nombre premier*, le sens de cette expression étant suffisamment clair d'après ce qui précède.

Pour trouver dans cet ordre d'idées une généralisation du théorème de Fermat, on doit rechercher s'il existe de même des *polynomes divisibles par un nombre composé quelconque* m ; ou, si l'on veut, des congruences dont le premier membre n'est pas identiquement nul (mod. m) et qui sont cependant vérifiées pour toute valeur entière de la variable.

Nous pouvons évidemment nous borner au cas où m est une puissance d'un nombre premier, car pour qu'un polynome soit divisible par $m = p^\alpha q^\beta r^\gamma$, il faut et il suffit qu'il soit divisible séparément par p^α, q^β, r^γ. En désignant par $P(x)$, $Q(x)$, $R(x)$ les expressions les plus générales des polynomes respectivement divisibles par p^α, q^β, r^γ, l'expression générale des polynomes divisibles par m sera visi-

(*) Bien entendu, il s'agit de la divisibilité suivant le module p.

blement

$$[P(x)+p^\alpha f(x)][Q(x)+q^\beta g(x)][R(x)+r^\gamma h(x)],$$

$f(x)$, $g(x)$, $h(x)$ désignant des polynomes quelconques.

Nous sommes ainsi amenés à rechercher les polynomes divisibles par p^α, p étant un nombre premier. Il est clair qu'il en est ainsi des α polynomes

$$\varphi_k(x) = p^{\alpha-k}(x^p - x)^k, \qquad (k = 1, 2, 3, \ldots \alpha),$$

et par suite en désignant par $f_k(x)$ des polynomes arbitraires, du polynome

$$\sum_1^\alpha f_k(x)\varphi_k(x).$$

Nous allons montrer, en supposant α inférieur à $p+1$, que le polynome ainsi obtenu (et ceux qui lui sont congrus suivant le module p^α) est le plus général des polynomes divisibles par p^α. Supposons cette proposition vraie jusqu'à une certaine valeur de α; nous allons voir qu'elle subsiste pour la valeur $\alpha+1$. Soit, en effet, $\alpha+1$ *étant au plus égal à* p,

$$\varphi(x) \equiv 0, \qquad (\text{mod. } p^{\alpha+1})$$

une congruence vérifiée quel que soit x; on a aussi, quel que soit x,

$$\varphi(x) \equiv 0, \qquad (\text{mod. } p^\alpha)$$

et par suite

$$\varphi(x) = \sum_1^\alpha f_k(x)\varphi_k(x) + p^\alpha f_0(x).$$

Soit x_0 une valeur quelconque de x; on a

$$x_0^p - x_0 = p\xi_0,$$

ξ_0 étant un entier déterminé; on en conclut aisément

$$(x_0+p\lambda)^p - (x_0+p\lambda) \equiv p(\xi_0 - \lambda) \qquad (\text{mod. } p^2).$$

Un calcul facile donne ensuite

$$\varphi_k(x_0+p\lambda) \equiv p^\alpha(\xi_0 - \lambda)^k \qquad (\text{mod. } p^{\alpha+1}).$$

On a donc

$$\varphi(x_0+p\lambda) \equiv p^\alpha\left[\sum_0^\alpha f_k(x_0+p\lambda)(\xi_0-\lambda)^k\right] \quad (\text{mod. } p^{\alpha+1}).$$

Or $$f_k(x_0+p\lambda)\equiv f_k(x_0) \qquad (\text{mod. } p).$$
Donc

$$\varphi(x_0+p\lambda)\equiv p^\alpha \sum_0^\alpha f_k(x_0)(\xi_0-\lambda)^k \qquad (\text{mod. } p^{\alpha+1}).$$

Donnons à x_0 une valeur fixe et faisons varier λ ; on verra que le polynome en $\xi_0-\lambda=\lambda_1$

$$\sum_0^\alpha f_k(x_0)\lambda_1^k$$

est divisible par le nombre premier p ; on a donc, puisque α est inférieur à p,

$$f_k(x_0)\equiv 0 \qquad (\text{mod. } p).$$

Comme x_0 est arbitraire, il en résulte

$$f_k(x)\equiv (x^p-x)g_k(x), \qquad (\text{mod. } p),$$
$$k=(0,1,2,\ldots,\alpha),$$

d'où l'on conclut aisément la proposition énoncée.

Si α dépassait p, il faudrait ajouter aux α polynomes $\varphi_k(x)$, les $\alpha-p$ polynomes

$$\psi_k(x)=[(x_p-x)^p-p^{p-1}(x_p-x)](x_p-x)^{k-1}p^{\alpha-p-k},$$
$$(k=1,2,3,\ldots,\alpha-p),$$

car l'expression entre crochets est manifestement divisible par p^{p+1}, quel que soit x, comme on le voit en posant $x^p-x=p\xi$.

On démontrerait, en suivant une marche tout à fait analogue, que si α est inférieur à $2p+2$, le polynome le plus général divisible par p^α est congru à

$$\sum_1^\alpha \varphi_k(x)f_k(x)+\sum_1^{\alpha-p}\psi_k(x)g_k(x),$$

les f et les g étant des polynomes arbitraires.

On aperçoit aisément comment on continuerait et on voit que le théorème de Fermat suffira toujours pour résoudre ces questions de divisibilité ; *il n'y a pas lieu d'en chercher de généralisation à ce point de vue*, à moins de considérer comme une généralisation le fait que l'expression

$$\varphi(x)=(x^p-x)^p-p^{p-1}(x^p-x),$$

est divisible par $p^{\nu+1}$; ou de même que

$$[\varphi'(x)]^{\nu} - p^{\nu^2-1}\varphi(x)$$

est divisible par $p^{\nu^2+\nu+1}$, etc.

En se servant *seulement* de ces diverses propositions et des théorèmes élémentaires suivants :

1° Si un nombre α divise deux nombres a et b, il divise $\lambda a + \mu b$;

2° Si les nombres α et β divisent respectivement a et b, $\alpha\beta$ divise ab ;

3° Un nombre divisible par deux autres premiers entre eux est divisible par leur produit,

on peut toujours arriver à reconnaître si un polynome donné est divisible par un nombre quelconque, et inversement, trouver tous les polynomes divisibles par un nombre donné.

NOTE II

SUR LES IMAGINAIRES DE GALOIS

1. Nous avons l'intention d'esquisser rapidement ici les principes de la théorie des imaginaires de Galois, en nous plaçant au point de vue qui nous semble avoir été adopté par ce grand géomètre.

Il est essentiel dans ce but de préciser les propriétés caractéristiques des entiers positifs lorsqu'on les envisage (mod. p), p étant un nombre premier, c'est-à-dire lorsqu'on néglige dans leur calcul les multiples de p ; c'est là ce qu'il est facile de faire. Nous savons en effet, qu'à ce point de vue :

Il existe p nombres distincts $0, 1, 2, \ldots, p-1$;

Un mode de composition de ces nombres, appelé *addition*, permet de passer de deux d'entre eux à un troisième *bien déterminé*, appelé leur somme, et cette composition possède les propriétés suivantes : 1° Elle est *associative*, c'est-à-dire que si le signe $(a+b)$ représente la somme des nombres a et b, l'on a, quels que soient les nombres a, b, c,

$$(a+(b+c)) = ((a+b)+c) ;$$

2° Elle est *commutative*, c'est-à-dire que l'on a, quels que soient les nombres a et b,

$$(a+b) = (b+a) ;$$

3° Si l'on compose un nombre a avec des nombres b et c différant entre eux, on obtient des résultats différant entre eux ; on peut donc conclure des égalités

$$a+b = d,$$
$$a+c = d$$

l'égalité
$$b = c.$$

Les propriétés qui précèdent sont *caractéristiques*, c'est-à-dire définissent complètement les entiers positifs (mod. p) ; nous allons

en effet établir que p symboles auxquels on attribue ces propriétés et celles-là seulement posséderont toutes les propriétés des entiers positifs (mod. p).

Soient a, b, ... l ces p symboles ; la suite : $a+j$, $b+j$, ..., $l+j$, où j désigne également un de ces symboles renfermera tous les éléments de la suite a, b, ..., l, puisqu'elle renferme p éléments distincts d'après la troisième propriété de l'addition. Il existe donc dans cette suite un élément, $c+j$ par exemple, qui est identique à j, et l'on conclut de là :

$$((c+j)+k) = (c+(j+k)) = (j+k),$$

quel que soit le symbole k, c'est-à-dire $(c+h) = h$ quel que soit h. Le symbole c est donc sans effet dans l'addition à gauche.

On montre de même qu'il existe un symbole c' qui est sans effet dans l'addition à droite, c'est-à-dire tel que l'on ait $(h+c') = h$ quel que soit le symbole h. Les deux relations

$$(c+c') = c, \qquad (c+c') = c'$$

établissent alors que c est identique à c'. On parvient d'ailleurs à cette même conclusion en invoquant la propriété commutative de l'addition :

$$(c+h) = (h+c) = h,$$

et ensuite la troisième propriété de l'addition pour établir qu'il n'existe qu'un symbole c tel que l'on ait $(h+c) = h$.

Nous désignerons par A_0 le symbole c auquel nous sommes ainsi parvenus.

Considérons maintenant un symbole quelconque a différent de c et la suite

$$(1) \qquad a, \qquad (a+a), \qquad ((a+a)+a), \qquad \ldots ;$$

les éléments de cette suite sont des symboles de la suite a, b, ..., l et par conséquent le nombre des symboles distincts qui sont ainsi obtenus est limité. Soit $q+1$ le rang du premier élément qui reproduit l'un des précédents ; l'élément reproduit est visiblement a et la suite (1) est périodique, ses termes se reproduisant de q en q. Nous allons montrer que q est nécessairement diviseur du nombre p des symboles distincts, ce qui exigera $p = q$, puisque p est premier et que l'élément $(a+a)$ est différent de a qui est égal à $(a+c)$.

Si l'on n'a pas en effet dans la suite (1) les p symboles donnés et si b désigne un symbole non obtenu, les symboles $(a+b)$, $((a+a)+b)$, $\Big(((a+a)+a)+b\Big)$, ..., qui font partie des $a, b, \ldots, l$, sont tous différents et sont aussi différents des précédents ; on déduirait par exemple de

$$(a+b) = (a+a)+a$$

l'égalité $(a+b) = a+(a+a)$, c'est-à-dire $b = (a+a)$. On obtient donc ainsi $2q$ symboles de la suite $a, b, \ldots, l$. Un raisonnement analogue montrerait, si l'on n'a pas épuisé ainsi cette suite, que d désignant un nouveau symbole, les symboles

$$(a+d), \qquad ((a+a)+d), \qquad \Big(((a+a)+a)+d\Big), \qquad \ldots,$$

sont encore différents et diffèrent de ceux déjà obtenus, et ainsi de suite. Il est clair qu'on épuise de cette manière tous les symboles $a, b, \ldots, l$ c'est-à-dire que p est multiple de q.

Dans le cas qui nous occupe où p est premier, on aura donc $p = q$.

Il résulte de là que *si l'on pose*

$$A_1 = a, \qquad A_2 = (a+a), \qquad A_3 = \big((a+a)+a\big), \qquad \ldots,$$

les symboles $A_0, A_1, A_2, \ldots, A_{p-1}$ *se composeront entre eux de la même manière que leurs indices* et par conséquent qu'à toutes les propriétés des entiers $0, 1, 2, \ldots, p-1$ correspondront les propriétés analogues pour les A dont les indices sont ces mêmes entiers. *Nous n'entendons pas autre chose en disant que les* A *sont ces entiers eux-mêmes*, regardant ainsi les entiers comme des *signes* ou symboles dont nous ne connaissons que les propriétés signalées plus haut.

Lorsque pour des éléments en nombre limité, l'on peut définir un mode de composition qui possède les propriétés suivantes :

1° De deux éléments quelconques on passe par la composition considérée à un troisième élément bien déterminé ;

2° La composition est associative ;

3° Un même élément composé avec des éléments différant entre eux donne des éléments différant entre eux,

on dit que *les éléments composés par ce mode de composition forment un groupe limité.*

Lorsqu'en outre la composition est *commutative*, le groupe est dit *abélien*.

Nous venons donc d'établir que les entiers $0, 1, 2, \ldots, p-1$ forment par addition un groupe abélien. Si l'on pose maintenant, a étant l'un de ces entiers :

$$a = 1.a, \qquad (a+a) = 2.a, \qquad (a+a)+a = 3.a, \qquad \ldots,$$

on définit ainsi un certain mode de composition des entiers 1 et a, 2 et a, 3 et a, etc., qu'on appelle multiplication et les propriétés de l'addition permettent d'établir les propriétés de ce nouveau mode qu'on peut résumer en disant :

Les entiers $1, 2, \ldots, p-1$ forment par multiplication un groupe abélien ;

L'entier 0 joue un rôle singulier et se reproduit dans la multiplication par un entier quelconque de la suite $0, 1, 2, \ldots, p-1$. Enfin la multiplication est distributive par rapport à l'addition, c'est-à-dire que l'on a $a.(b+c) = a.b + a.c$.

Les relations qui donnent, lorsqu'on connaît deux éléments d'un groupe, le résultat de leur composition, s'appellent *relations fondamentales* du groupe ; il est clair que les propriétés des entiers positifs (mod. p) peuvent toutes se déduire de la connaissance de ces relations fondamentales pour l'addition : l'existence de la multiplication et ses propriétés en sont par exemple des conséquences.

Ainsi pour définir le calcul des entiers (mod. 5) il suffit de donner la première des deux tables de composition suivantes :

	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Ces tables peuvent être appelées *tables de structure* des groupes formés par nos symboles pour les deux modes de composition : addition et multiplication.

2. Nous sommes maintenant en mesure de montrer comment peut se faire l'introduction dans le calcul des imaginaires congruentielles de Galois.

Soit $f(x) \equiv 0 \pmod{p}$ une congruence irréductible de degré n; nous savons qu'il n'existe aucun élément de la suite $0, 1, 2, \ldots, p-1$ qui vérifie cette congruence. En d'autres termes, lorsqu'on astreint x à figurer parmi les symboles $0, 1, 2, \ldots, p-1$, la congruence $f(x) \equiv 0 \pmod{p}$ n'a aucune racine. Il est naturel de penser qu'en restreignant convenablement le nombre des conditions imposées au symbole x, il pourra exister dans l'ensemble des symboles satisfaisant à ces conditions des racines de cette congruence. Les conditions à imposer au symbole x peuvent d'ailleurs être quelconques, pourvu que le polynome $f(x)$ soit par là entièrement défini lorsqu'on donne x puisque le second membre 0 est un symbole bien déterminé. Parmi les divers systèmes de conditions que l'on peut adopter, Galois a choisi l'un des plus simples qui consiste à supposer que *le symbole x se compose avec lui-même et avec les entiers $0, 1, 2, \ldots, p-1$ suivant deux modes différents qui possèdent les propriétés respectives de l'addition et de la multiplication de ces entiers.*

Il résulte de là que si x vérifie la congruence $f(x) \equiv 0 \pmod{p}$, les fonctions entières de x, fonctions qui sont définies d'une manière précise par les hypothèses, sont toutes représentées et une fois seulement dans la suite des polynomes $a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$, où les a sont des éléments quelconques de la suite $0, 1, 2, \ldots, p-1$. On montre alors qu'il est possible de définir pour ces éléments parmi lesquels figurent les entiers $0, 1, 2, \ldots, p-1$, deux modes de composition qui possèdent les propriétés respectives de l'addition et de la multiplication des entiers, c'est-à-dire que l'on peut construire les tables de structure des groupes abéliens correspondants.

Considérons par exemple la congruence irréductible $x^2 + 1 \equiv 0 \pmod{3}$ et désignons par i un symbole assujetti à posséder les modes de composition indiqués et à vérifier cette congruence : $i^2 + 1 \equiv 0 \pmod{3}$.

Les seules fonctions qui peuvent résulter de la composition de i avec lui-même et avec les entiers par les deux modes supposés sont les fonctions entières de i à coefficients entiers ; chacune d'elles est

d'ailleurs identique à un polynome du premier degré de la forme $ai+b$, où a et b sont pris dans les entiers 0, 1, 2, ainsi qu'il résulte de la relation $i^2+1 \equiv 0$ (mod. 3); il suffit donc d'étudier ces derniers éléments.

On peut d'ailleurs établir facilement que *d'une manière générale* si x est un symbole qui se compose avec lui-même et avec les entiers suivant deux modes qui possèdent les propriété respectives de l'addition et de la multiplication, les polynomes entiers en x se composent entre eux par deux modes qui possèdent ces mêmes propriétés. Il suffit de poser ici

$$(a+bx)+(a'+b'x) = (a+a')+(b+b')x,$$
$$(a+bx)(a'+b'x) = aa'+(ba'+ab')x+bb'x^2$$

pour le vérifier immédiatement.

Si l'on a égard à l'hypothèse faite sur le symbole i : $i^2+1 \equiv 0$ (mod. 3), on en conclut que les deux tables d'addition et de multiplication des symboles $ai+b$ peuvent être construites sans qu'il se présente de contradiction. Si nous posons, par exemple,

$$ai+b = A_{3a+b},$$

ces tables de structure sont les suivantes :

Addition :

	A_0	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8
A_0	A_0	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8
A_1	A_1	A_2	A_0	A_4	A_5	A_3	A_7	A_8	A_6
A_2	A_2	A_0	A_1	A_5	A_3	A_4	A_8	A_6	A_7
A_3	A_3	A_4	A_5	A_6	A_7	A_8	A_0	A_1	A_2
A_4	A_4	A_5	A_3	A_7	A_8	A_6	A_1	A_2	A_0
A_5	A_5	A_3	A_4	A_8	A_6	A_7	A_2	A_0	A_1
A_6	A_6	A_7	A_8	A_0	A_1	A_2	A_3	A_4	A_5
A_7	A_7	A_8	A_6	A_1	A_2	A_0	A_4	A_5	A_3
A_8	A_8	A_6	A_7	A_2	A_0	A_1	A_5	A_3	A_4

Multiplication :

	A_0	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8
A_0	A_0	A_0	A_0	A_0	A_0	A_0	A_0	A_0	A_0
A_1	A_0	A_1	A_2	A_3	A_4	A_6	A_6	A_7	A_8
A_2	A_0	A_2	A_1	A_6	A_8	A_7	A_3	A_5	A_4
A_3	A_0	A_3	A_6	A_2	A_5	A_8	A_1	A_4	A_7
A_4	A_0	A_4	A_8	A_5	A_6	A_1	A_7	A_2	A_3
A_5	A_0	A_5	A_7	A_8	A_1	A_3	A_4	A_6	A_2
A_6	A_0	A_6	A_3	A_1	A_7	A_4	A_2	A_8	A_5
A_7	A_0	A_7	A_5	A_4	A_2	A_6	A_8	A_3	A_1
A_8	A_0	A_8	A_4	A_7	A_3	A_2	A_5	A_1	A_6

La construction de ces tables *qui suffisent à définir les éléments* $ai + b$, *au même titre que la table d'addition définit les entiers*, montre d'une manière évidente qu'il existe effectivement un symbole i possédant toutes les propriétés requises et qui vérifie la congruence $i^2 + 1 \equiv 0 \pmod{3}$.

Ajoutons qu'en rangeant les symboles dans un autre ordre on peut donner à la table de multiplication la forme suivante :

	A_0	A_1	A_5	A_3	A_8	A_2	A_7	A_6	A_4
A_0	A_0	A_0	A_0	A_0	A_0	A_0	A_0	A_0	A_0
A_1	A_0	A_1	A_5	A_3	A_8	A_2	A_7	A_6	A_4
A_5	A_0	A_5	A_3	A_8	A_2	A_7	A_6	A_4	A_1
A_3	A_0	A_3	A_8	A_2	A_7	A_6	A_4	A_1	A_5
A_8	A_0	A_8	A_2	A_7	A_6	A_4	A_1	A_5	A_3
A_2	A_0	A_2	A_7	A_6	A_4	A_1	A_5	A_3	A_8
A_7	A_0	A_7	A_6	A_4	A_1	A_5	A_3	A_8	A_2
A_6	A_0	A_6	A_4	A_1	A_5	A_3	A_8	A_2	A_7
A_4	A_0	A_4	A_1	A_6	A_3	A_8	A_2	A_7	A_6

On en verrait facilement la raison.

La possibilité de définir logiquement les imaginaires de Galois étant ainsi établie, il serait facile de développer leur étude en mettant en évidence les analogies qu'elle présente d'une part avec l'étude des entiers (mod. p) et d'autre part avec la théorie des entiers algébriques dans un domaine $[\xi]$. Notre dessein n'étant pas de reprendre à ce nouveau point de vue des résultats déjà connus, nous renverrons le lecteur à ce qui a été dit sur cet objet dans la *Théorie des nombres*.

BAR-LE-DUC. — IMPRIMERIE COMTE-JACQUET

